HACKER INSIDE

TOP SECRET

FILE 1

HACKER INSIDE

TOP SECRET



EDITORA AFILIADA

HACKER INSIDE

TOP SECRET



EDITORA TERRA

HACKER INSIDE
TOP SECRET

Editor: Flavio Tâmega
Redatores: Sérgio Danin, Ally Junio
Capa: Marcus Vinicius Barcelos Pires
Projeto Gráfico: Cristiano Pricinote, Marcus Vinicius Barcelos Pires
Tipografia Downcome: misprinted type
Revisão: Cléssia Poliana

ISBN 85-7491-166-6

Diretor: Jales Júnior Martins Borges
Gerente de Produto: Cássio Rodrigues
Coordenadora de Marketing: Simone Ticks
Gerente Comercial: Anderson Kleber
Logística: Romualdo Brandão

Editora Gráfica Terra Ltda.
Divisão Comercial
Av. Caiapó, 758 – Setor Santa Genoveva
CEP: 74672-400 – Goiânia-GO – Brasil
Tel.: (62) 4005-9000 – Fax: (62) 207-1666
Televendas: (62) 4005-9090
E-mail: redacao@editoraterra.com.br
Home Page: www.editoraterra.com.br

SUMÁRIO

CAPÍTULO 1

VISÃO GERAL

- Noções de Rede
- Protocolos
- Portas

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

1. Conceitos de Rede

Em tecnologia de informação, uma rede (o termo rede refere-se, ao longo do curso, à rede de computadores) é definida como uma série de pontos ou nós interligados. As redes podem estar conectadas a outras redes e conter sub-redes. Um computador ligado a outro já é considerado uma rede. Podemos dizer que é a interligação de dispositivos que se comunicam, como o sistema de telefonia, caixas eletrônicos 24 horas (bancos) e outros mais.

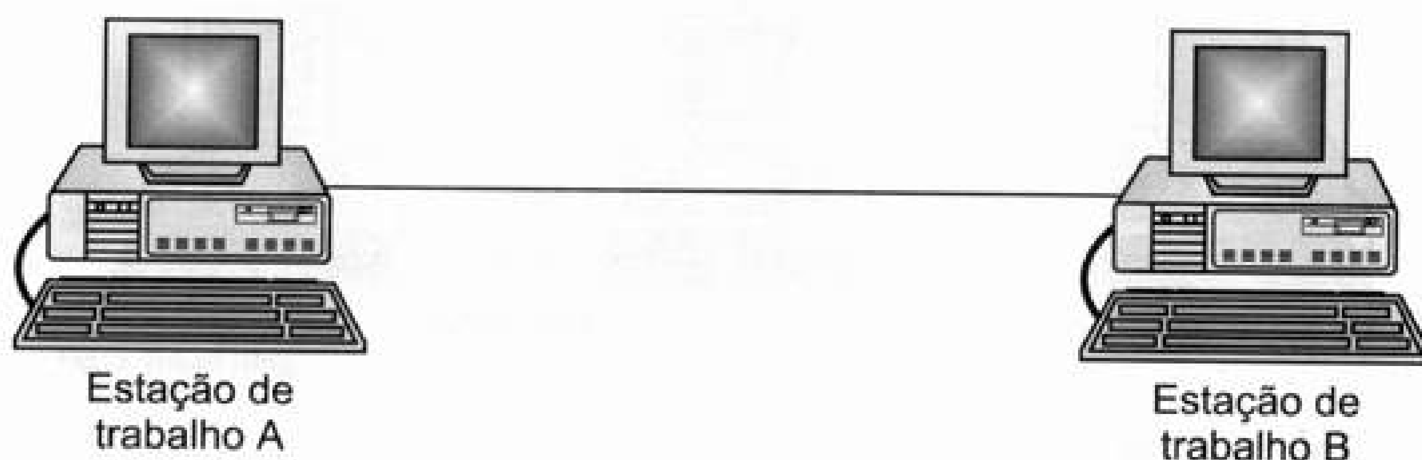


Fig. 1. Rede Interligado dois computadores.

Comumente em uma rede de computadores, dizemos que as estações de trabalho são os pontos e os nós são os hubs ("conectores"), existem também outros dispositivos que fazem parte da rede, mas nunca fugindo à regra de ser uma série de pontos ou nós interligados.

Ethernet

A Ethernet é o padrão mais utilizado em redes locais (LAN). Em uma Ethernet, pode-se utilizar tanto cabo coaxial quanto cabo par trançado e até mesmo nenhum cabo como nas novas tecnologias de redes sem fio (wireless). Seu funcionamento parte do princípio de todos os micros compartilharem uma mesma linha (cabo), independente da topologia física utilizada, isto significa que, quando uma linha estiver em uso, nenhum outro micro poderá enviar informações até que a linha esteja livre.

É como se chamássemos um número telefônico ocupado e ligássemos até desocupar.

Na Ethernet, é utilizado o protocolo[1] CSMA/CD (Carrier Sense Multiple Access/Collision Detect), um ponto fraco é que ele não utiliza nenhum tipo de prioridade, ou seja, todos os micros fazem a checagem da linha até que ela esteja livre, se dois ou mais micros tentarem enviar dados ao mesmo tempo, ocorrerá uma colisão e nenhuma das placas conseguirá transmitir os dados.

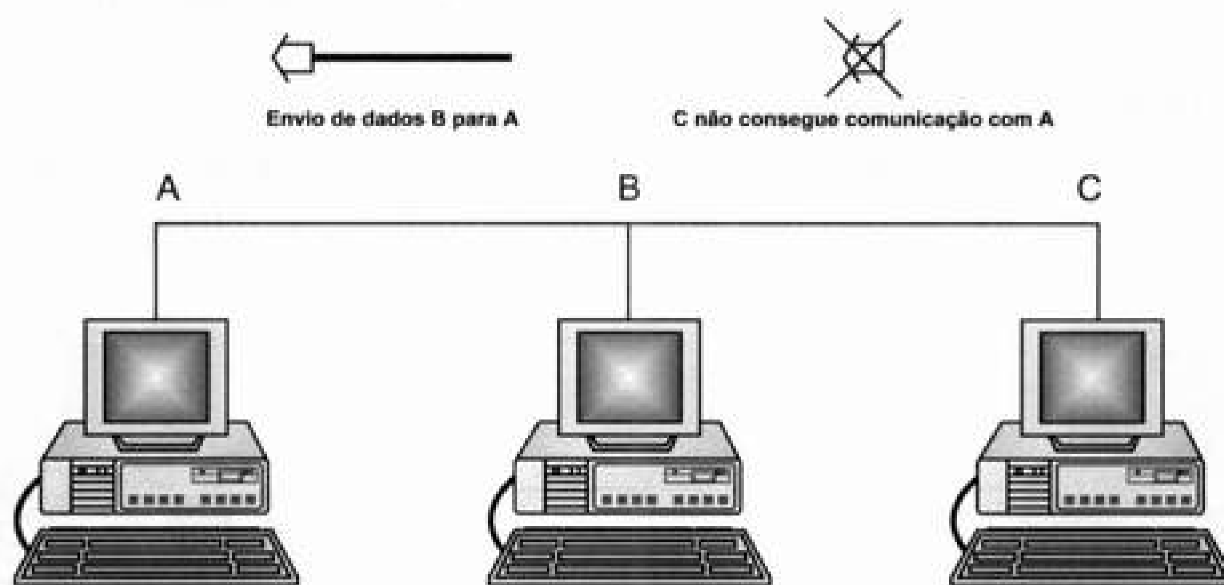


Fig. 2. GSMD/CD.

Token Ring

No padrão Token Ring, como no Ethernet, a linha de transmissão deve estar livre para que os dados trafeguem, a diferença é que, no Token Ring, cada máquina possui um tempo certo de enviar um pacote de dados, não existindo colisões.

A topologia física é em forma de anel, daí o nome Ring, os dados são transferidos em 4 ou 16 megabits por segundo.

---

*1 - **Protocolo** – Conjunto de regras que deve ser obedecido para que se possa transmitir uma informação de um dispositivo a outro.*

Veja, a seguir, algumas características da Token Ring:

1.º Um pacote com sinais (Token) em branco transita continuamente na rede (anel).

2.º Quando um micro tem algo a enviar, ele simplesmente insere os dados dentro desta "ficha", incluindo a identificação, ou seja, para qual máquina os dados estão endereçados.

3.º As fichas são examinadas por cada uma das máquinas. Se alguma for a máquina destinatária, ela copia os dados e "zera" a ficha novamente.

4.º Quando a ficha volta ao remetente, ele verifica que o dado chegou ao destinatário e, então, deixa a ficha circular novamente, pronta para que mais dados sejam transmitidos.

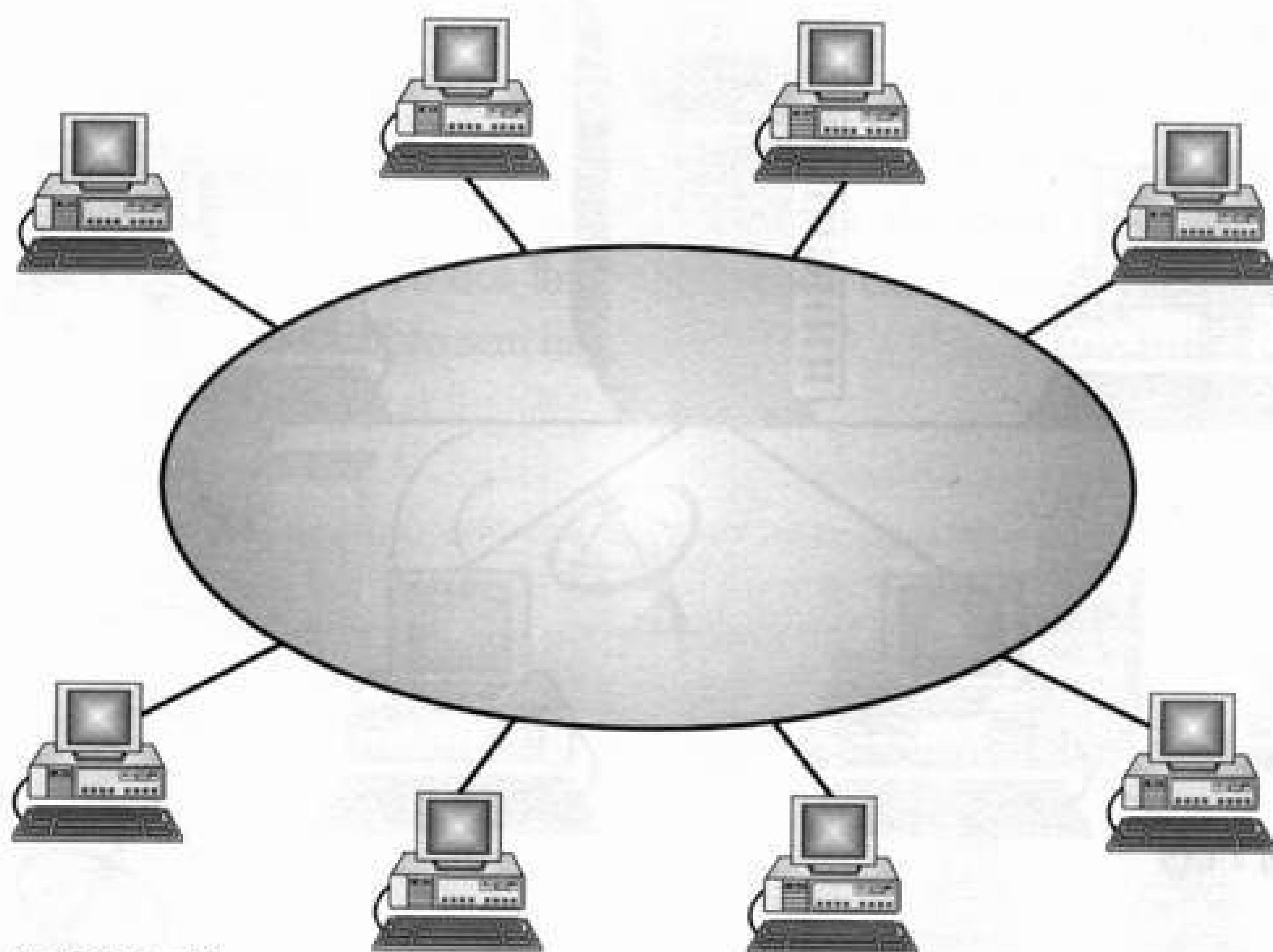


Fig. 3. Token Ring.

As redes também podem ser caracterizadas em termos de área abrangente, por exemplo:

LAN (Local Area Networks)

É um grupo de computadores e periféricos que compartilha, em uma mesma linha de comunicação, os recursos de um servidor, como processador e discos rígidos.

Um bom exemplo é uma rede de uma pequena empresa, em que as estações de trabalho compartilham uma única máquina (servidor).

Geralmente, no servidor, estão guardados dados que são acessados por diversas estações de trabalho. A LAN pode ser utilizada tanto em uma rede pequena (doméstica), com dois ou três micros conectados, como em redes maiores por centenas de usuários.

Em redes domésticas, é comum utilizar as próprias estações de trabalho como "servidores", podendo compartilhar alguns recursos, como processador, espaço em disco, conexões, aplicativos e muito mais.

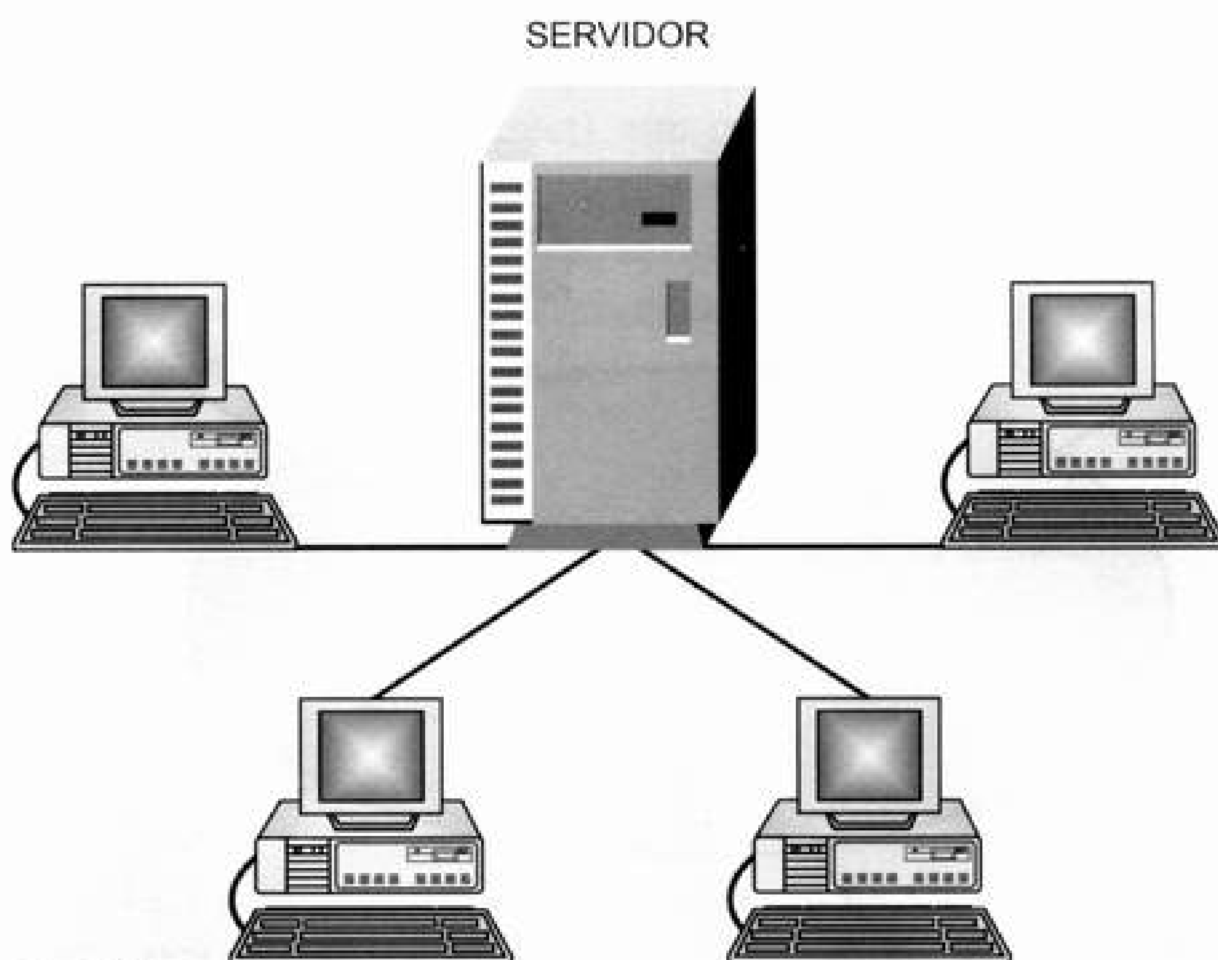


Fig. 4. LAN.

MAN (Metropolitan Area Networks)

A MAN é uma rede que interliga estações em uma área geográfica maior do que a coberta por uma LAN, também compartilhando recursos destas máquinas, mas, ao mesmo tempo, é menor que a área de abrangência de uma WAN. Na verdade, MAN é a conexão de uma rede LAN com outra. Exemplo: Campus universitário, onde prédios com LANs distintas comunicam-se.

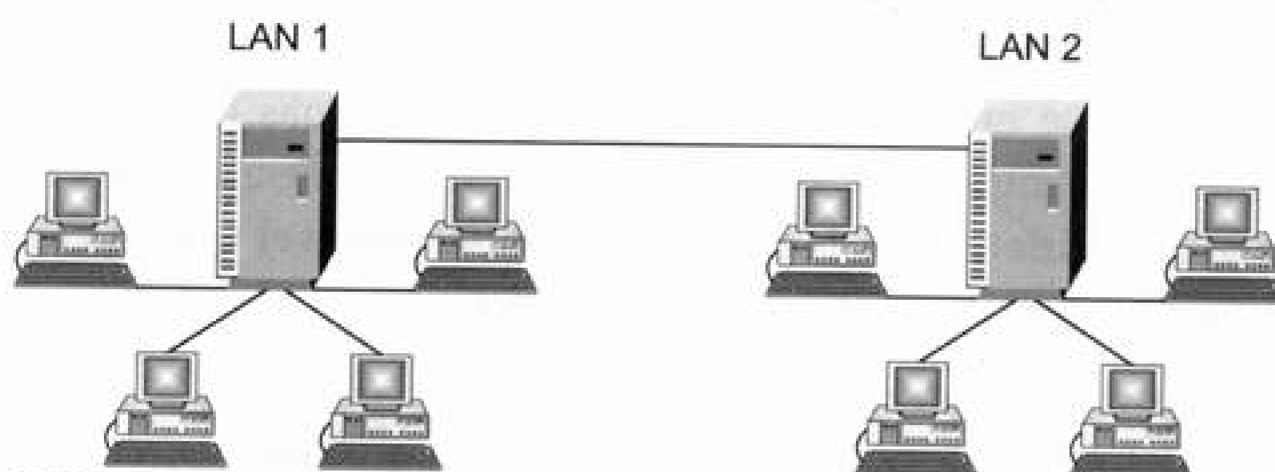


Fig. 5. MAN.

WAN (Wide Area Networks)

Pode-se dizer que a WAN é uma rede de telecomunicações geograficamente dispersada. Geralmente, uma WAN tem linhas de conexão privadas que são compartilhadas por outras redes. Uma rede também pode ser caracterizada pelo tipo de transmissão de dados, pelo que trafega na rede (voz ou dados), por quem pode utiliza a rede (pública ou privada), pela natureza da conexão (discada, dedicada, conexão virtual etc.) e pelo tipo físico dos links (fibra ótica, cabo coaxial, par trançado, wireless (comunicação sem fio).

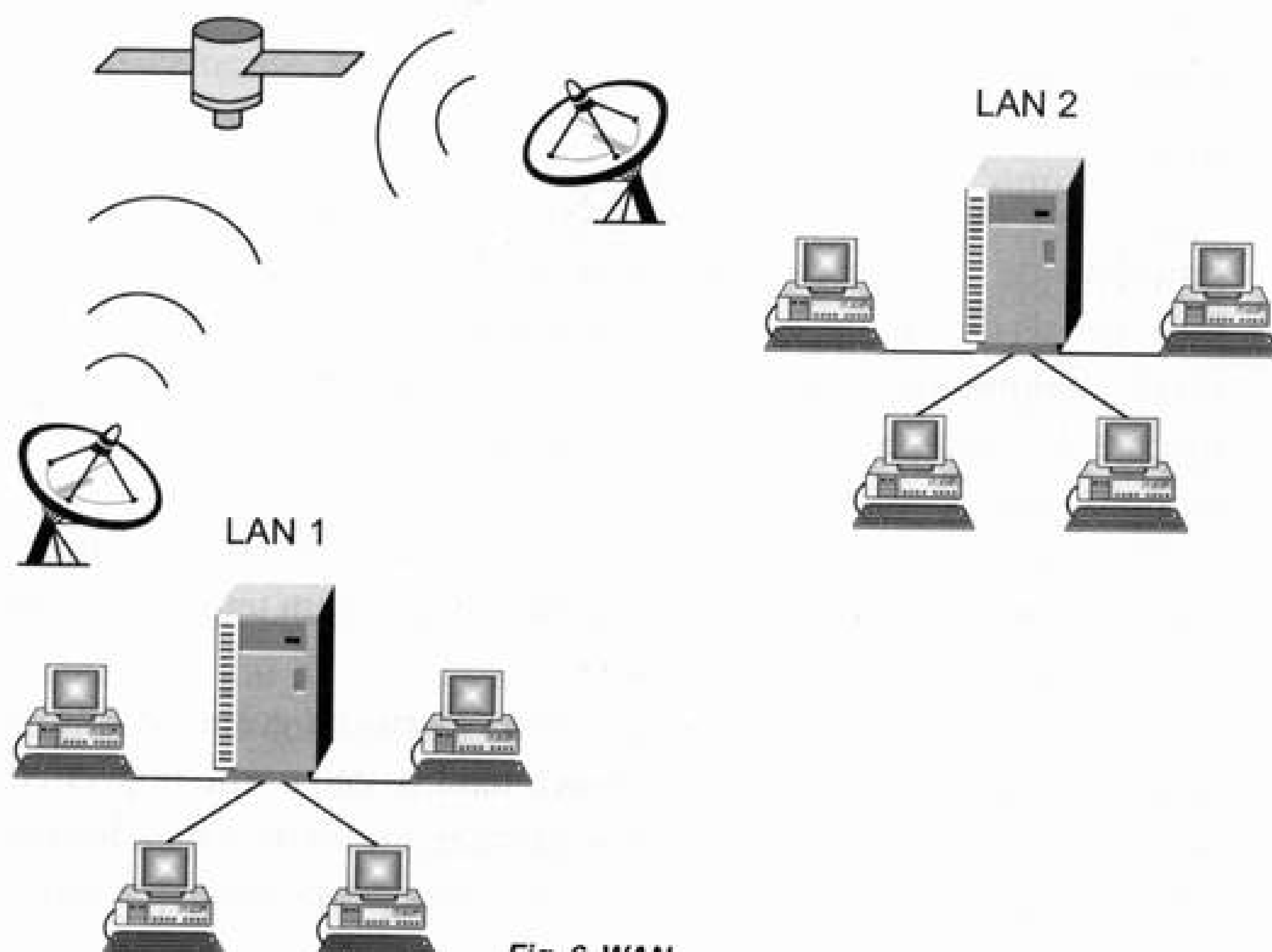


Fig. 6. WAN.

2. Internet/Intranet/Extranet

Muito se ouve sobre Internet e Intranet, mas poucos sabem a diferença entre um e outro. O princípio é o mesmo, mas existem algumas diferenças. Na sua empresa, é possível que você utilize uma Intranet e pense estar na Internet.

– História da Internet

Ela foi criada pela ARPA (*Advanced Research Projects Agency*), um órgão do governo dos Estados Unidos, em 1969, e primeiramente foi conhecida como ARPANET. O objetivo inicial era que fosse criada uma conexão entre pesquisadores de uma universidade com outras e que assim pudessem trocar informações por meio do próprio computador. Uma das vantagens era que os dados poderiam trafegar em mais de uma direção, ou seja, se houvesse algum desastre ambiental, ou mesmo uma guerra que destruísse a conexão com alguma rede (neste caso uma universidade), não afetaria as outras, sendo que os dados poderiam continuar trafegando entre os demais pontos.

Hoje a Internet é pública, cooperativa, não existe uma empresa que administre a Internet. Ela é acessada por milhares de usuários em qualquer região do planeta.

Internet

Às vezes, também é chamada de Net. Ela é um gigantesco conjunto mundial que interliga computadores por linhas de comunicação (telefone, canais de satélite, cabos etc). É a rede das redes, na qual, o usuário de qualquer computador, se tiver permissão, pode conseguir informações de outros computadores, ou mesmo interagir direto com outro computador.

Os recursos que a Internet fornece são inúmeros, como: conversas via texto, transmissão de arquivos, som e imagem em tempo real, compartilhamento de recursos e muito mais.

A Internet é um dos mais expressivos canais de comunicação, um fato até então não imaginado há pouco tempo. Isto é real, hoje em dia, acompanhamos tudo quase ao vivo, guerras, fatos em países distantes, transmissão de rádio e até conversas ao vivo com pessoas que vivem a milhares de quilômetros de nós.



Fig. 7. Internet.

Fisicamente, a Internet utiliza os recursos das redes de telecomunicações públicas, o que a distingue tecnicamente é que um grupo de protocolos, chamado de TCP/IP (Transmission Control Protocol/ Internet Protocol), é utilizado. Daí vem a Intranet que é uma adaptação da tecnologia da Internet e, também, utiliza o protocolo TCP/IP.

Para a maioria dos usuários, o correio eletrônico (E-mail) praticamente substituiu o serviço postal comum. Atualmente, o e-mail é o serviço mais utilizado na Internet, além disso, recentemente, foi criada uma tecnologia capaz de permitir conversas (voz) em tempo real (voz sobre IP).

Um outro serviço muito utilizado é a Web, que vem do inglês *World Wide Web*, ou a "grande teia mundial", também chamada WWW e muitas vezes confundida com a própria Internet.

Utilizando a Web, você tem acesso a milhares de páginas com informações, a "navegação" é feita a partir de um software, chamado de Browser ou navegador, os mais utilizados são o Internet Explorer, que já vem no Windows, e o Netscape Navigator.

Na Web, é possível visualizar páginas que contenham somente texto, outras com som, vídeo, realidade virtual e muito mais.

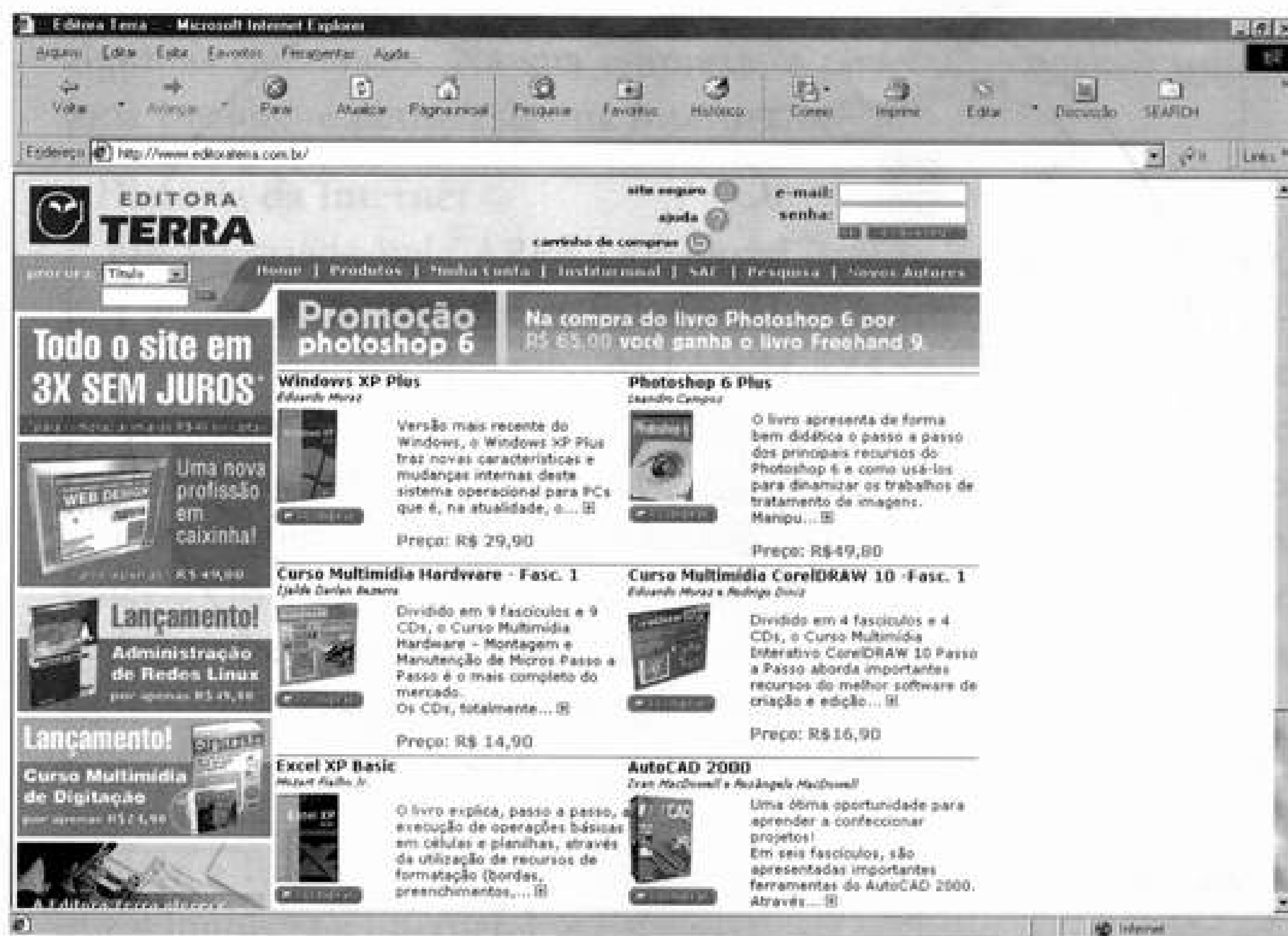


Fig. 8. Browser (Acesso a uma página web).

Intranet

É uma rede privada, geralmente dentro de uma empresa, que consiste em uma ou algumas LANs interconectadas. Comumente, uma Intranet faz as conexões com a Internet por meio de um ou mais *gateways*. O objetivo principal de uma Intranet é compartilhar informações e dados de uma empresa entre seus funcionários, ou seja, só acessa quem for cadastrado na Intranet. Outros usuários que estiverem na Internet não têm acesso a ela.

Como na Internet, a Intranet utiliza o protocolo TCP/IP e pode conter os mesmos recursos da Internet.

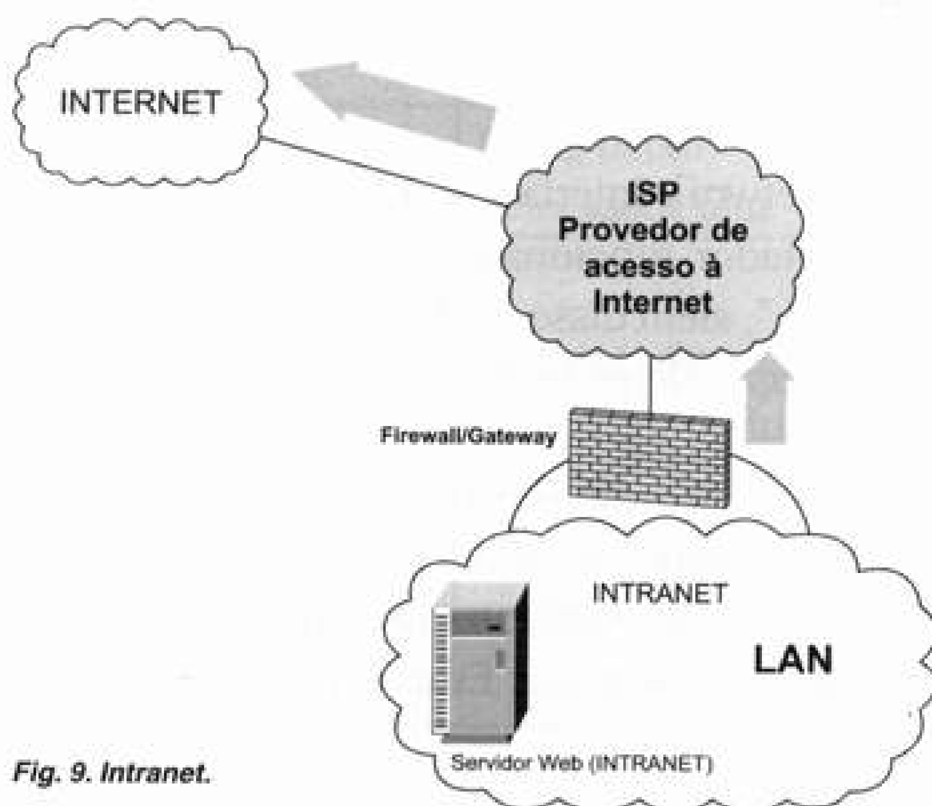


Fig. 9. Intranet.

Extranet

A Extranet é uma extensão da Intranet, mas estendida para usuários que estiverem fora da empresa (Intranet). Uma Extranet requer segurança e privacidade, para isto, deve-se implantar um *Firewall*, encripitação de pacotes e outras medidas de segurança.

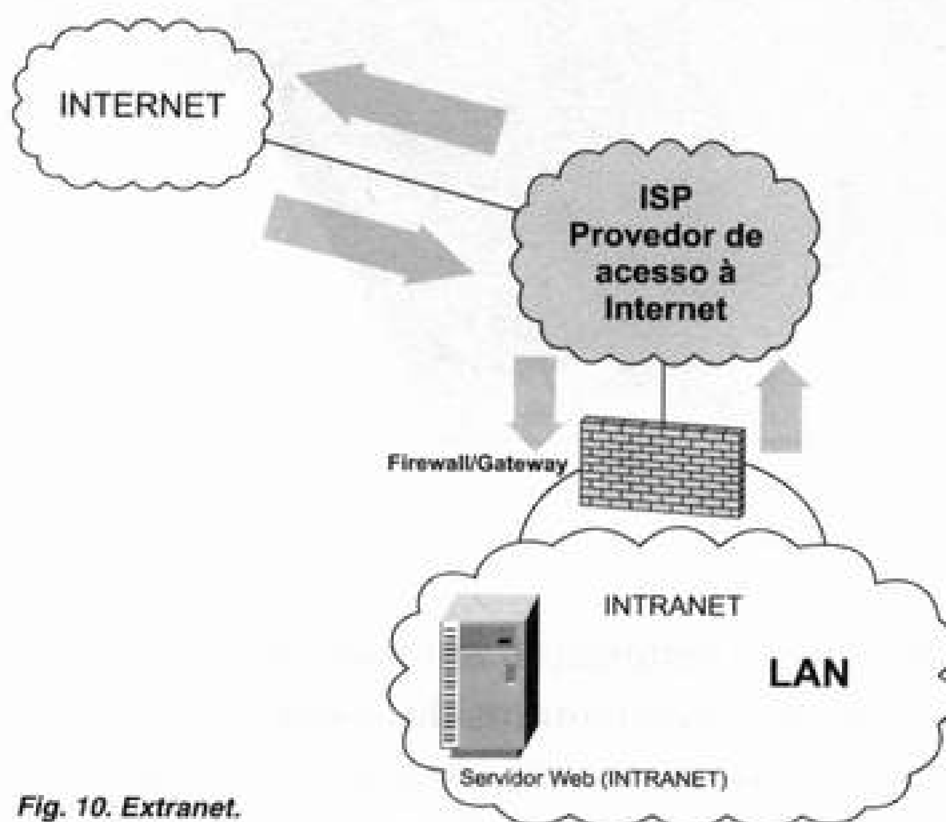


Fig. 10. Extranet.

3. Componentes

Placa de Rede

A placa de rede (NIC – Network Interface Card) é uma placa que, ao ser instalada em um computador, funciona como um meio de comunicação entre o micro e a "rede", além disso, a placa de rede desempenha outras funções, como correção de erros e verificação de integridade dos dados recebidos.

A placa deve ser escolhida de acordo com a tecnologia de transmissão (arquitetura de rede), como Ethernet ou Token Ring, não se esquecendo de verificar a compatibilidade com o cabeamento utilizado.

As placas mais utilizadas são: as placas Ethernet 10/100 com saída para cabo par trançado.

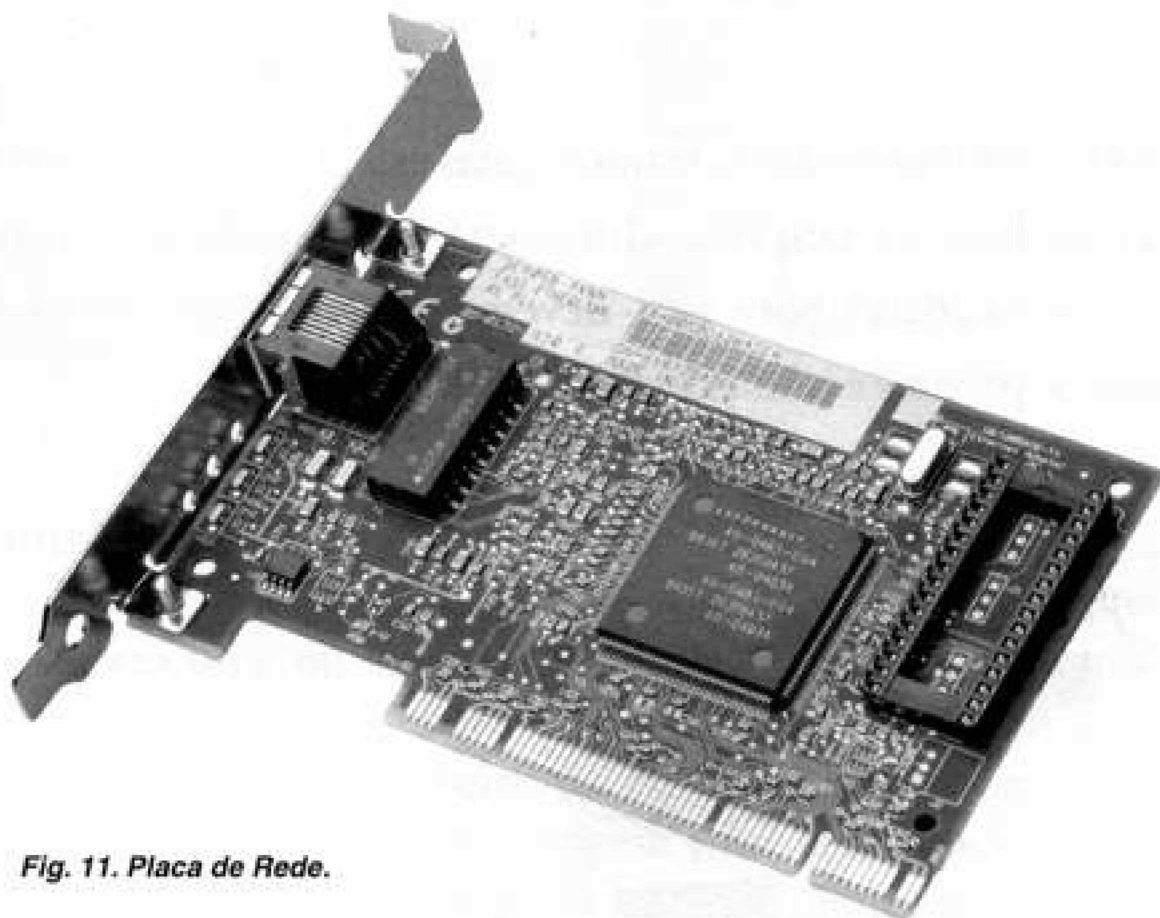


Fig. 11. Placa de Rede.

Cabo de Rede

Os cabos de rede fazem a comunicação entre as interfaces de rede, como placas de rede, *switches*, *hubs* e outros dispositivos. Os mais utilizados atualmente são os cabos par trançado e coaxial, além deles, é possível conectar os dispositivos por fibra ótica, ondas de rádio (sem utilização de cabos, tecnologia conhecida como wireless), entre outros. Cada um tem suas vantagens e limitações.

Topologia	Vantagem	Desvantagem
Cabos (coaxial ou par trançado)	Preço baixo Velocidade alta	Tempo de Montagem
Wireless (sem cabos)	Mobilidade Instalação rápida e simples	Preço elevado. Velocidade diminui à medida que os dispositivos se distanciam do Gateway.



Fig. 12. Par trançado.



Fig. 13. Cabo coaxial.

Hub

Dispositivo que une cabos de comunicação em um ponto central, fornecendo uma via comum de comunicação a todos os dispositivos. O Hub funciona como um repetidor, ao contrário do *Switch*, ele não consegue saber o endereço do destinatário e, então, envia os dados para todos os micros. Não é muito aconselhado utilizar com muitas máquinas, pois pode gerar um "gargalo" nas linhas.

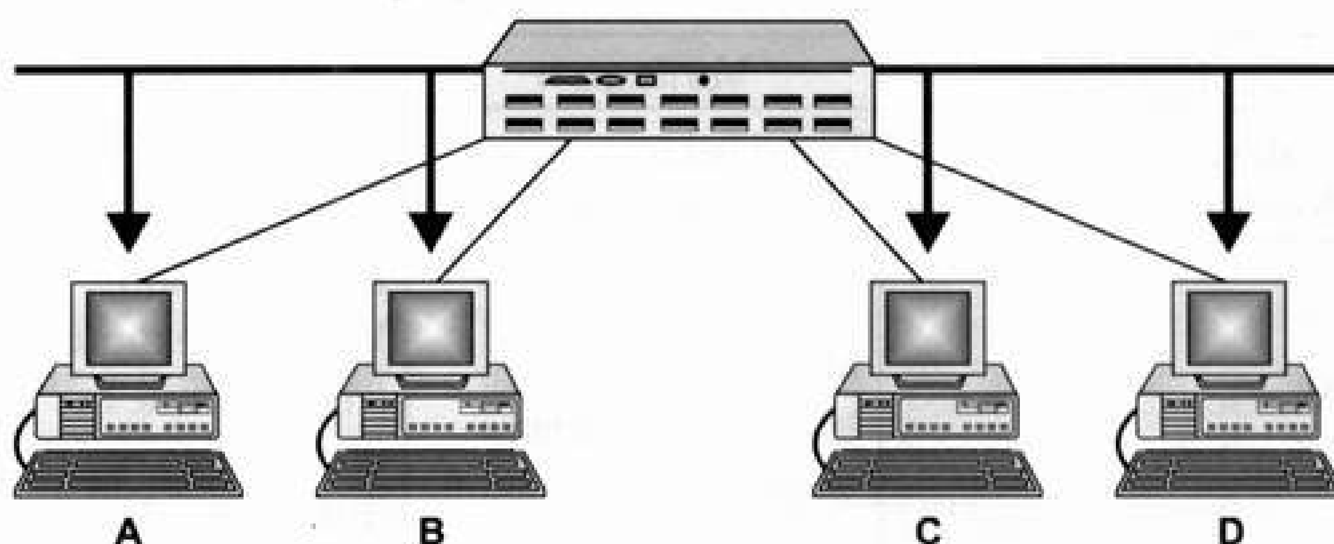


Fig. 14. HUB.

Switch

Ao contrário do Hub, o Switch é um comutador, ou seja, ele recebe as linhas de transmissão e, então, determina para onde os dados serão enviados, não provocando "congestionamentos" na saída dos dados, veja figura 15.

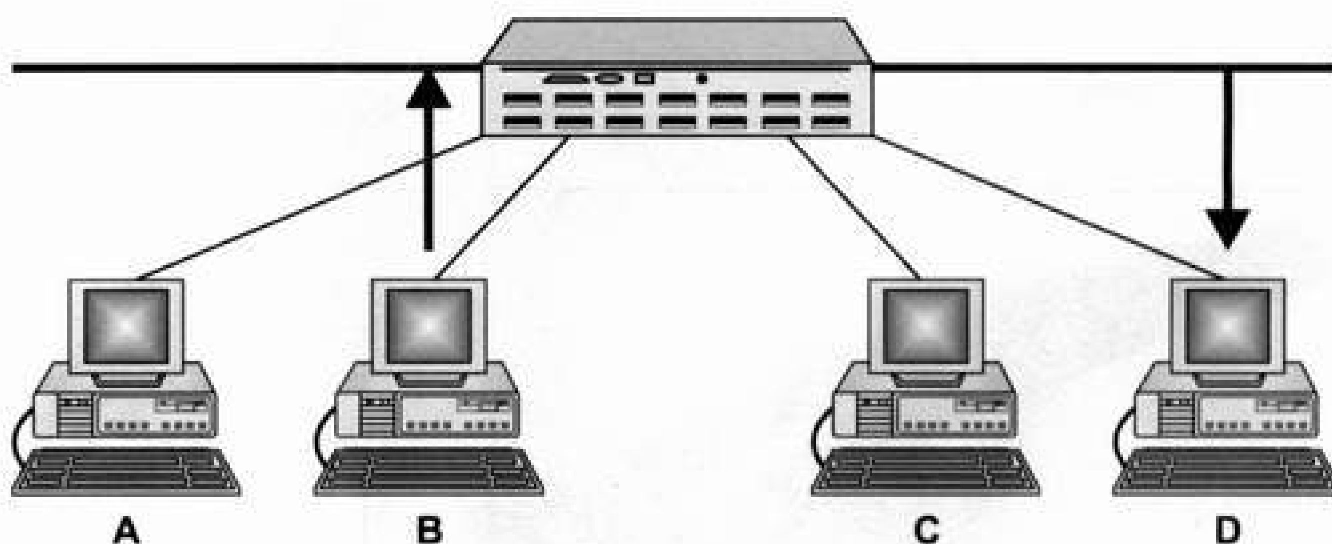


Fig. 15. Switch.

Roteador

Em redes, o roteador pode ser um dispositivo físico ou, então, um software. Sua função é determinar o próximo ponto para onde um pacote de dados será enviado. O roteador deverá estar pelo menos conectado a duas redes para, daí, poder "decidir" o caminho de cada pacote de dados, veja figura 16.



Fig. 16. Gateway.

Gateway

O mesmo que roteador. Sistema que interliga duas ou mais redes, com diferentes protocolos de comunicação, de modo que seja possível transferir informações entre elas. A Internet é formada por inúmeros roteadores interligados, cada um serve como meio de conexão para uma rede distinta.

Firewall

É ele quem "protege" uma rede, traduzindo significa "muro de fogo". Nada mais é do que um software ou um componente dedicado, que protege a rede contra invasões externas e acessos não autorizados. Atualmente, o Firewall está deixando de fazer parte apenas das redes de empresas, para proteger, também, redes domésticas.

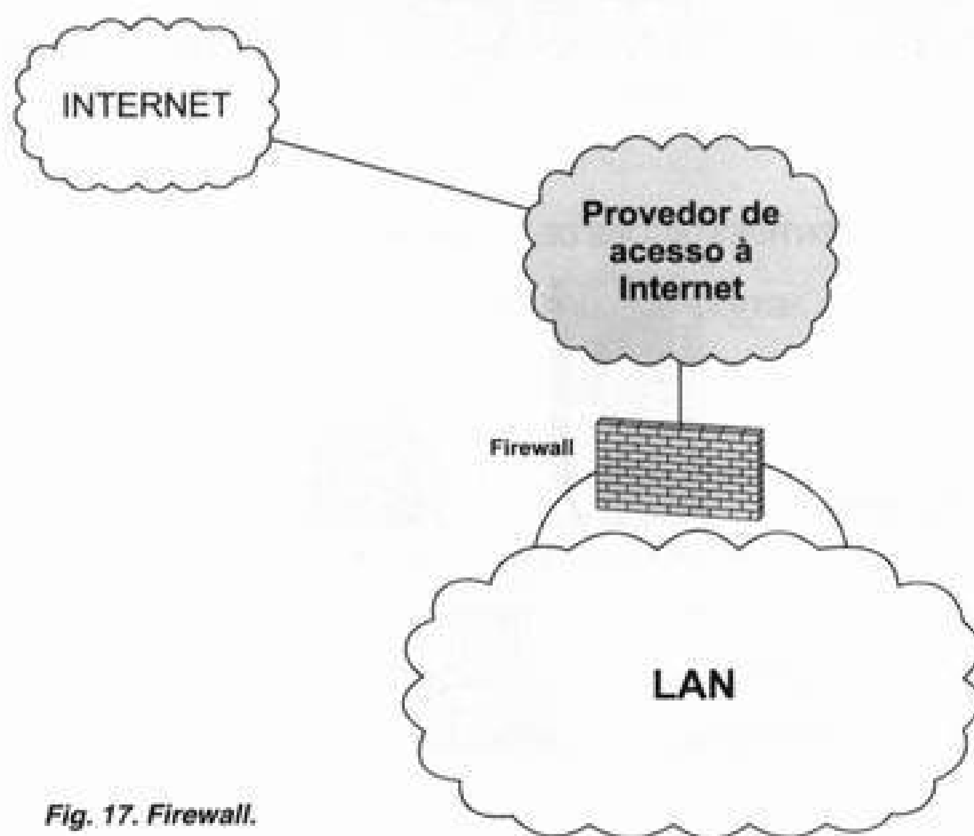


Fig. 17. Firewall.

Servidor

Máquina que compartilha recursos com outros computadores na rede. Podendo compartilhar espaço em disco, conexões, periféricos.

Geralmente, é um computador mais robusto e não deve ser utilizado, também, como estação de trabalho.

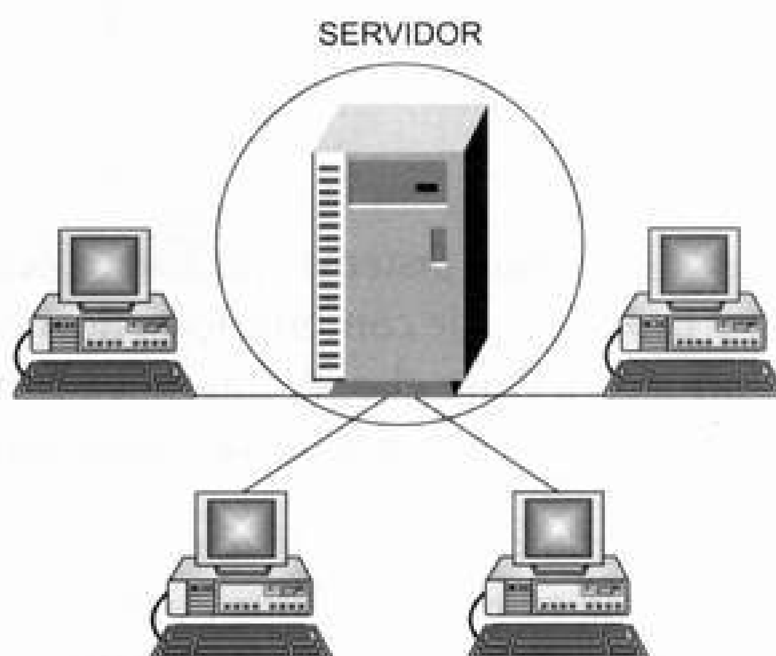


Fig. 18. Servidor.

Cliente

São as *workstations* (estações de trabalho), máquinas que acessam os recursos de um servidor. O cliente pode acessar os recursos disponibilizados no servidor, caso haja necessidade, o cliente deve ser autenticado pelo servidor, veja figura 19.



Fig. 19. Cliente.

Sistema Operacional

Para as estações de trabalho, deve ser utilizado qualquer sistema operacional que tenha suporte à rede (Ex.: Windows 95/98/Me, Windows

XP professional); para os servidores, Windows 2000, Sistemas operacionais com recurso de servidores (Ex.: Windows 2003/Linux/Unix).

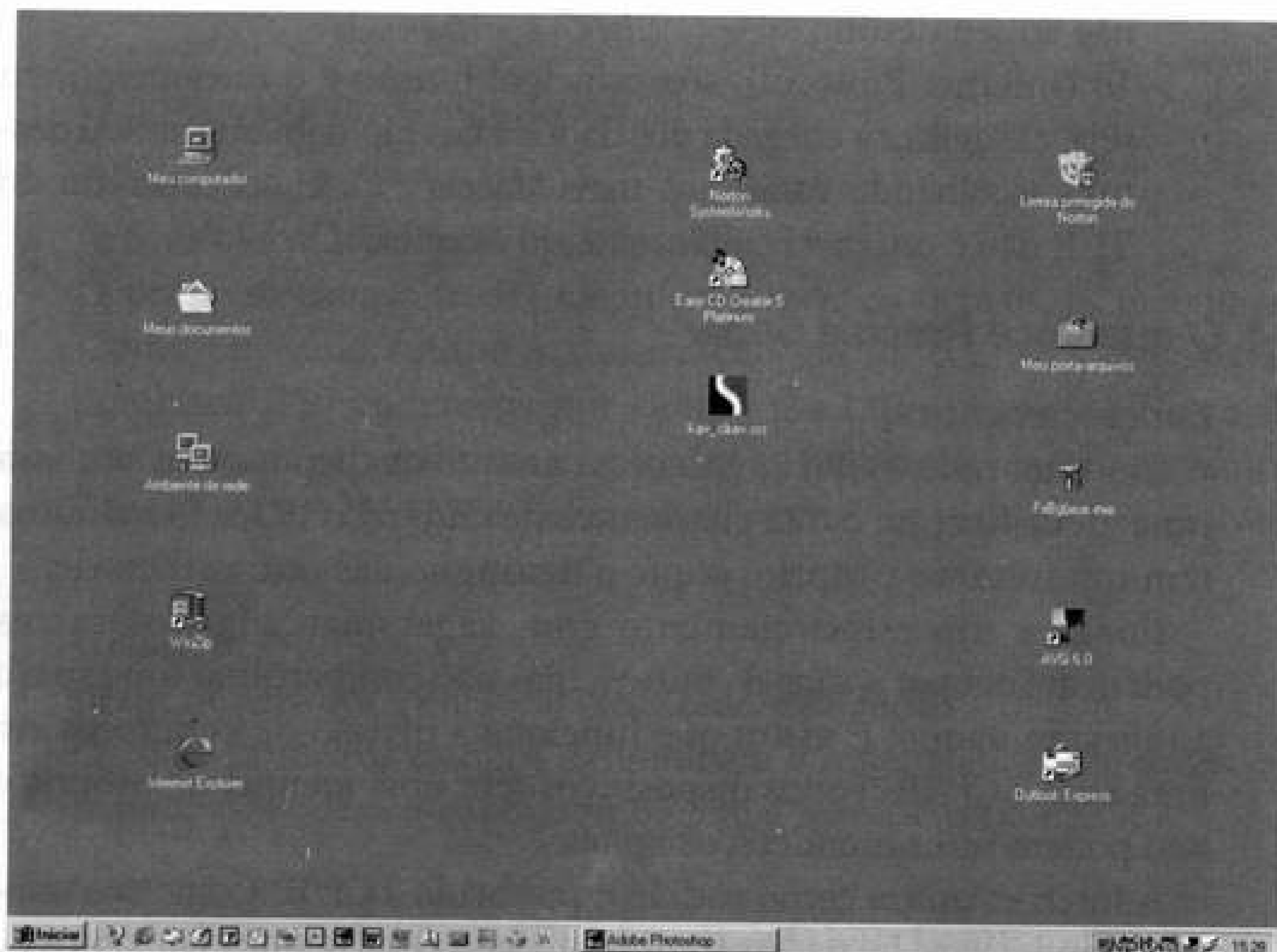


Fig. 20. Máquina utilizando o Windows 98.

Protocolo

O protocolo é um conjunto de regras que deve ser obedecido para que se possa transmitir uma informação de um dispositivo para outro. Os protocolos também são utilizados em outros tipos de comunicações, como telefonia.

Existe uma grande variedade de protocolos, cada um tem suas vantagens e suas desvantagens, por exemplo: Uns são mais simples para se implantar, mais rápidos e mais utilizados, como o TCP/IP, que é o padrão da Internet.

O TCP/IP é regido pelas normas e padrões internacionais, sendo ele compatível com a maioria dos sistemas operacionais.

O TCP/IP é, na verdade, uma suíte, ou seja, um conjunto de protocolos e regras, dentre os quais, destacamos o TCP e o IP:

- TCP (Transmission Control Protocol) usa um conjunto de regras para troca de mensagens, ou seja, é a camada de transporte. O protocolo TCP é quem verifica se um determinado dado chegou ou não ao seu destino.
- IP (Internet Protocol), sua principal função é o roteamento, ou seja, ele agiliza a chegada dos dados mais rapidamente ao seu destino escolhendo caminhos mais "fáceis". O IP, ao contrário do TCP, não é um protocolo orientado à conexão.

4. O que Você Precisa Saber

Endereçamento IP

Em uma rede TCP/IP, é necessário que os dispositivos tenham uma identificação, o que chamamos de endereço IP, cada máquina tem um número próprio, o que a distingue das outras na rede.

Imagine um estacionamento com vagas marcadas, os carros podem até ocupar a vaga de outros, mas não compartilhar um espaço ao mesmo tempo. É assim que funciona a divisão de endereços em uma rede TCP/IP. Todos dispositivos têm uma identidade própria e não podem utilizar endereços iguais.

A Internet utiliza como padrão o protocolo TCP/IP. Como são muitos os endereços, foi necessária a criação de grupos, que chamamos de "classes" para facilitar a distribuição dos endereços IP.

Em uma rede local, a comunicação com a Internet é feita por um ponto específico (Gateway), portanto, não se preocupe em "escolher" endereços IPs diferentes dos que já estão em uso na Internet, pois a comunicação entre as máquinas de sua rede será somente local.

A única que deverá ter um IP válido na Internet é o *Gateway*, pois é ele quem "conversa" com a Internet. Mas, quanto a isso, não se preocupe, pois este endereço é dado pelo seu *ISP* (provedor de acesso à Internet).

Deve-se adotar uma classe de acordo com a dimensão da rede que irá configurar, veja, a seguir, uma comparação entre as classes que podem ser utilizadas e, então, selecione a que melhor se adaptar às suas necessidades:

Classe A – Para redes de grande porte, é possível conectar até 16.777.216 dispositivos (256^3).

Classe B – Para redes de médio porte, é possível conectar até 65.536 dispositivos (256^2).

Classe C – Para redes de pequeno porte, é possível conectar até 256 dispositivos (256^1).

O que os números significam

Classe A

network.local.local.local (rede.local.local.local)

O primeiro campo (rede) identifica a rede; os demais, as máquinas. Como em cada campo a numeração vai de 0 a 255, é possível combinar 256 endereços por campo (1+255). Como na classe A, três campos servem para identificar as máquinas, então, elevamos 256 a 3: (256*256*256) e chegamos ao total de 16.777.216 possíveis combinações.

Classe B

network.network.local.local (rede.rede.local.local)

Os dois primeiros campos denominam a rede; os dois seguintes, as máquinas. Podemos configurar 65.536 dispositivos (256*256).

Classe C

network.network.network.local (rede.rede.rede.local)

Neste caso, somente o último campo identifica as máquinas, sendo possível configurar até 256 dispositivos.

Existem ainda as classes D e E, não são muito utilizadas.

A "família" TCP/IP

Como dissemos, anteriormente, o TCP/IP é um conjunto de protocolos, dentre eles, estão alguns muito familiares aos internautas, como o *FTP, HTTP, SMTP, TELNET*, entre outros. Cada um tem uma função específica. Confira:

FTP (File Transfer Protocol)

É a maneira mais simples de troca de arquivos entre computadores na Internet. O FTP é muito utilizado por desenvolvedores Web para enviar arquivos para o servidor, também, quando fazemos download (baixar arquivo) da Internet.

Para o usuário, o FTP pode ser utilizado a partir de linhas de comando em uma tela do MS-DOS, navegadores (browsers), como o

Internet Explorer e Netscape Navigator, ou por programas específicos para FTP.

Muitas vezes, você acessa ou baixa arquivos em uma página Web por meio de FTP. Nos navegadores, o tipo do servidor pode ser facilmente percebido quando aparece "ftp://" ao invés de "http://" na barra de endereços.

HTTP (Hypertext Transfer Protocol)

É um conjunto de regras para a troca de arquivos (texto, imagens, som, vídeo e outros arquivos multimídia) na Web (World Wide Web/ WWW).

Todo servidor Web contém além dos arquivos (páginas web, banco de dados etc.) um programa próprio que "espera" a requisição do endereço Web e, então, envia os dados para o cliente quando estes são pedidos. O seu navegador é o cliente Web, é ele quem envia o pedido de requisição e, depois, somente interpreta os arquivos "abrindo" uma página Web.

SMTP (Simple Mail Transfer Protocol)

O "protocolo de transferência de correio", e como o próprio nome indica: é o responsável pelo envio e recebimento dos e-mails, entretanto, tem a limitação de só "guardar" as mensagens no servidor, não enviando diretamente à caixa de mensagem do usuário. Para enviá-las, é necessário utilizar outro protocolo, como o POP ou IMAP (Internet Message Access Protocol), estes sim fazem a intermediação das mensagens que estiverem no servidor para a caixa de mensagens do usuário.

Exemplo:

1. Uma mensagem é enviada para o seu e-mail: usuario@email.com.br
2. O servidor de e-mail responsável pelo domínio email. com.br recebe esta mensagem utilizando o protocolo SMTP, então, guarda a mensagem no próprio servidor.
3. Você utiliza um cliente de e-mail (Outlook, Eudora, Outlook Express...) e checa suas mensagens direto no servidor, apontando para um endereço POP.

Em outras palavras, os usuários, por meio de um cliente de e-mail, uti-

lizam o protocolo SMTP para envio e o POP ou IMAP para recebimento das mensagens. Note que o POP ou o IMAP é só utilizado pelo cliente, ou seja, serve só para a comunicação servidor/cliente.

Telnet

O Telnet é utilizado para acessar uma outra máquina, desde que você tenha permissão de acesso. Mais tecnicamente, o Telnet é acessado por linha de comando e funciona atrelado ao protocolo TCP/IP, diferente do que acontece quando se utiliza o protocolo HTTP ou FTP, no qual, você acessa a máquina remota como se fosse um usuário local.

Portas

Em computadores e dispositivos de telecomunicações, a porta é geralmente um local para se conectar em um soquete (tomada) ou algum tipo de plug. Tipicamente, um computador pessoal dispõe de uma ou mais portas serial e uma porta paralela. A porta serial suporta transmissão seqüencial, enquanto a porta paralela faz transmissão múltipla de dados.

Em programação, a porta vem a ser uma conexão lógica. O cliente, pelo protocolo TCP/IP, especifica o servidor (programa) em uma rede. Aplicações de alto nível que utilizam o TCP/IP como protocolo Web, HTTP, têm portas com números determinados. Estas portas são denominadas "portas conhecidas" e são determinadas pelo IANA (Internet Assigned Numbers Authority).

O número das portas varia de 0 até 65536. Portas que variam de 0 a 1024 são reservadas para alguns serviços. Para utilizar o serviço HTTP, a porta 80 é definida como padrão e não precisa ser mencionada ao se fazer uma busca por URL.

Confira, a seguir, as portas mais utilizadas por padrão em alguns serviços:

Portas para serviços Internet

Serviço	Porta	Descrição
SSH	22	Acesso remoto (shell)
HTTP	80	HyperText Transfer Protocol (navegação Web)
LDAP	389	Acesso a serviço de diretório
MS Netmeeting	1024	Videoconferência
Timbuktu	1417-1420	Controle e acesso remoto
SLP	427	Service Location Protocol (MacOS)
HTTPs	443	HTTP seguro
ULP	522	User Location Protocol (Microsoft)
Quick Time 4	RTSP	Streaming de áudio e vídeo
RTSP	554	Real Time Streaming Protocol
NNTPs	563	News – segura
IPP	631	Serviço de impressão remota, via Internet
LDAPs	636	LDAP segura
Doom	666	Jogo Doom via rede
SOCKS	1080	Proxy
VocalTec Internet Phone	1490, 6670, 25793	Videoconferência
Xing Stream Works	1558 (UDP)	Streaming de vídeo
PPTP	1723	VPN
MS ICCP	1731	Audio call control (Microsoft)
MS Netshow	1755	Streaming de vídeo
MSN Messenger	1863	Instant messenging
Glimpserver	2001	Ferramenta de busca
Squid	3128	Proxy web
Mirabilis ICQ	Dinâmica >=1024	Instant messenging

Blizzard / Battle.net	4000, 6112-6119	Jogos em rede
GlobalChat client, server	4020	Programa de bate-papo
Yahoo Messenger – Voice Chat	5000-5001	Comunicação via voz
Yahoo Messenger – messages	5050	Instant messenging
Yahoo Messenger – webcams	5100	Vídeo chat
AOL Instant Messenger	5190	Instant messenging
AOL ICQ	5190, dinâmico >=1024	Instant messenging
Pcanywhere	5631	Ferramenta de acesso e controle remoto
VNC	5800+,5900+	Ferramenta de acesso e controle remoto
Netscape Conference	6498, 6502	Audioconferência
Common IRC	6665-6669	Internet Relay Chat – Bate-Papo
VDOLive	7000	Streaming de vídeo
Real Audio & Video	RTSP, 7070	Streaming de áudio e vídeo
CU-seeme	7648, 7649, LDAP	Videoconferência
HTTP	8000, 8001, 8080	
Quake	26000	Jogo em rede
MSN Gaming zone	28800-29000	Jogo em rede
DirectX Gaming	47624, 2300-2400	Jogos em rede

Capítulo 2

FUNDAMENTOS

- Termos Utilizados

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

Nas organizações modernas, as redes de computadores têm crescido a uma velocidade espantosa. Em contra partida, os controles de segurança precisam ser adequados às novas tecnologias empregadas. A falta de ferramentas para monitoração de rede dificulta o processo de implementação de um verdadeiro sistema de segurança digital.

O crescimento desordenado de compartilhamento de informações é um ponto crítico em qualquer rede pois o sigilo dessas informações é o que garante sua integridade.

O ser humano está sempre à procura de desafios, hackers, crackers e sua turma são os campeões na busca por brechas digitais. Você aprende o que eles podem fazer para prejudicar um computador pessoal, ou até mesmo acessar informações sigilosas de uma empresa e também como se proteger. Na verdade, podemos separar esses invasores digitais em dois grandes grupos: aqueles que visam a apenas acessar os sistemas e aqueles que pretendem destruir ou usar informações em benefício próprio. Veja, a seguir, os principais termos utilizados pelos hackers e crackers.

1. Termos

1.1. Hackers

São Invasores que apenas descobrem as brechas digitais, invadem um sistema para pesquisá-lo sem autorização, para estudos ou para

provar alguma teoria, invadindo a privacidade alheia. Os hackers não visam a prejudicar ou se aproveitar do que estão fazendo em benefício próprio, geralmente são os "eticamente corretos", ou *White Hat* (chapéu branco).

O hacker é geralmente um programador habilidoso que tem conhecimento aprofundado de sistemas operacionais e linguagens de programação de baixo nível. São pessoas comprometidas com a produção e distribuição do conhecimento de tecnologia.

1.2. Crackers

Já os crackers têm outra motivação, seu objetivo é a invasão, a destruição ou a apropriação indevida de informações sigilosas. Podemos caracterizar um cracker por suas ações de cunho destrutivo e malicioso.

Os crackers são aqueles que roubam números de cartão de crédito e os utilizam para fazer compras, se apossam de informações de clientes de uma empresa e até mesmo para vender estes dados. Possuem quase sempre as mesmas habilidades dos hackers, porém as utilizam de forma negativa.

1.3. Lammers

O lammer é normalmente definido como um iniciante que se empenha em descobrir comandos e programas que servem para ludibriar instituições e em fazer de outros lammers seu principal alvo, passando horas diante de um computador.

Lammers, gostam de se promover e adoram se intitular hacker diante dos outros. Na verdade, não possuem conhecimento aprofundado de linguagens de programação, nem do funcionamento exato do sistema operacional, muito menos dos protocolos de redes. São geralmente discriminados entre hackers e crackers.

1.4. Newbie

Newbie é um novato na rede, agora que está descobrindo o que a Internet pode oferecer a ele, às vezes, faz perguntas e se mete em lugares que não deveria. Mas aquele cara que entra num chat com nick de *newbie* é um "espertinho" querendo dar uma de ingênuo. Por mais que seja ingênuo, ele não vai entrar na sala com isso estampado na cara.

1.5. Wannbe

Wannbe é um principiante que aprendeu a usar alguns programas prontos (no jargão hacker, receitas de bolo) para descobrir senhas ou invadir sistemas, entrou num provedor de "fundo de quintal" e pensa que vai conseguir entrar nos computadores da Nasa.

1.6. Phreaker

Tem ótimos conhecimentos de telefonia, inclusive consegue fazer chamadas internacionais sem pagar, o que lhe permite desenvolver seus ataques a partir de um servidor de outro país (telefone).

1.7. Sniffer

O *sniffer* é um programa para captura de informações destinadas a uma outra máquina.

1.8. Spoofing

O spoofing do IP envolve o fornecimento de informações falsas sobre uma pessoa ou sobre a identidade de um host para obter acesso não-autorizado a sistemas e/ou aos sistemas que eles fornecem. Ainda, interfere na forma como um cliente e um servidor estabelecem uma conexão. Apesar de poder ocorrer com diversos protocolos específicos, o do IP é o mais conhecido dentre todos os ataques de spoofing.

A primeira etapa de um ataque é identificar duas máquinas de destino, as quais chamaremos de A e B. Na maioria dos casos, uma máquina terá um relacionamento confiável com a outra, Com isso, o ataque tentará explorá-lo. Uma vez que os sistemas de destino tenham sido identificados, o violador tentará estabelecer uma conexão com a máquina B de forma que B acredite haver uma conexão com A, quando, na realidade, a conexão é com a máquina do violador, que chamaremos de X. Isso é feito pela criação de uma mensagem falsa (uma mensagem criada na máquina X, mas que contém o endereço de origem de A) solicitando uma conexão com B. Mediante o recebimento dessa mensagem, B responderá com uma mensagem semelhante que reconhece a solicitação e estabelece números de seqüência.

O spoofing do IP, como acabamos de descrever, é uma estratégia desajeitada e entediante. No entanto, uma análise recente revelou a existência de ferramentas capazes de executar ataque em menos de 20 segundos.

O spoofing de IP é uma ameaça perigosa, cada vez maior, mas, por sorte, é relativamente fácil criar mecanismos de proteção contra ela. A melhor defesa é configurar roteadores de modo a rejeitar qualquer pacote recebido cuja origem alegada seja um host da rede interna.

1.9. Trojans

A lenda do cavalo de Tróia diz que um grande cavalo de madeira foi ofertado pelos gregos aos troianos, como sinal de que estavam desistindo da guerra. Mas, o cavalo escondia, no seu interior, um grupo de soldados gregos que esperaram a noite e abriram os portões da cidade de Tróia para o exército grego que a invadiu e dominou.

Um *trojan* é um programa que oculta o seu objetivo sob uma camuflagem de outro programa útil ou inofensivo. Funciona como um servidor de rede (SERVER) e tem um outro programa "comparsa", que funciona como cliente (CLIENT).

O server fica instalado no computador da vítima e o cliente no computador do cracker. Se ambos estiverem na internet, o cracker pode estabelecer uma conexão direta (cliente-servidor), não monitorada e imperceptível com o Server (vítima) por um backdoor. Assim, estes programas oferecem grande risco para a máquina infectada, pois se tem quase que total controle sobre a máquina remota, podendo acessar todos os arquivos, ou mesmo apagá-los.

1.10. Newsgroup

Grupos de discussão da Usenet (rede de mensagens da Internet que usa o Network News Transfer Protocol (NNTP)). Cada newsgroup (grupo de discussão) trata de um assunto (tema) específico, desde alienígenas no Novo México até culinária tailandesa.

Os grupos estão organizados em hierarquias de tópicos. A primeira parte do nome do grupo designa a categoria geral a que ele pertence. As partes seguintes são as subcategorias. As categorias gerais são: news (notícias, avisos), rec (lazer, entretenimento), soc (sociedade), sci (ciência), comp (computação), entre muitas outras.

Os usuários podem responder a mensagens postadas, introduzir novas mensagens e até criar um novo grupo de discussão (newsgroup). Assim, um grande repositório de troca de informações está nos diversos newsgroups espalhados pelo mundo. De maneira geral, os

hackers freqüentam assiduamente essas listas de discussão, trocando todos os tipos de informações e experiências.

1.11. Firewalls

Em redes de computadores, firewalls são barreiras interpostas entre a rede privada e a externa com a finalidade de evitar intrusos (ataques); ou seja, são mecanismos (dispositivos) de segurança que protegem os recursos de hardware e software da empresa dos perigos (ameaças) aos quais o sistema está exposto.

Estes mecanismos de segurança são baseados em hardware e software e seguem a política de segurança estabelecida pela empresa. Basicamente, um firewall trabalha junto a um roteador ou a uma máquina responsável pelo roteamento. Assim, ele examina cada pacote de rede determinando qual é sua origem e seu destino. Geralmente, o firewall é instalado em uma máquina separada do resto da rede corporativa, desta maneira, cria-se uma barreira entre a rede interna e a rede externa.

1.12. IRC

O IRC (Internet Relay Chat) é um serviço da Internet para bate-bapo, um dos precursores dos conhecidos Instant messengers. O IRC também é muito utilizado pelos hackers por ser uma maneira simples e rápida para trocar informações e experiências.

1.13. Exploits

Exploits são programas geralmente feitos em linguagem C que exploram a vulnerabilidade de programas e sistemas para ganhar acesso root ou administrador, muitos dos exploits são para sistemas Linux. São scripts em C que são executados no servidor de maneira que causam estouro de pilha em algum software ou serviço, estes estouros são chamados de Stack Overflow, Heap Overflow.

1.14. Worms

Um worm é um vírus que se auto-reproduz sem alterar o conteúdo dos arquivos infectados. Ele reside na memória ativa do computador, permitindo assim uma grande disseminação do vírus. Os worms se alocam em locais de difícil acesso no sistema operacional, assim, ficam

imperceptíveis ao usuário. Outra característica deles é que estão sempre mudando de nome e infectando outros arquivos.

1.15. DoS (Denial of Service)

DoS, ou negação de serviço, é um ataque em que um usuário ou um servidor é impedido de usar os serviços e recursos que ele normalmente teria. Por exemplo, um web site pode ficar fora do ar por um ataque DoS. Este tipo de ataque pode também destruir arquivos e programas. Na verdade, funciona por envio de um grande número de pacotes para o servidor que queremos derrubar, como o servidor não está preparado para interpretar toda essa demanda, ele encerra sua operação. Então conseqüentemente, negando o acesso aos seus serviços.

1.16. Criptografia (ou Encriptação)

Encriptação é alterar os dados de tal forma que passe a ser sem sentido e mesmo ininteligível a qualquer um que não possua a chave secreta para transformar aqueles dados em forma legível.

A criptografia possibilita que você guarde importantes informações ou as transmita por redes inseguras (como a Internet) de tal modo que a informação não pode ser lida a não ser pelas pessoas que se pretende. Inclui técnicas de micropontos, combinação de textos com imagens e várias outras maneiras matemáticas de garantir o sigilo dos dados armazenados e transmitidos.

Criptografia pode ser forte ou fraca, como se explicou acima. A força é medida de acordo com o tempo e os recursos que se exige para recuperar os dados. O resultado forte é o texto (dado) cifrado que é muito difícil decifrar sem possuir ferramenta apropriada para decodificação.

1.17. Vírus

São programas desenvolvidos para alterar nociva e clandestinamente softwares instalados em um computador, têm comportamento semelhante ao dos vírus biológico: multiplicam-se, precisam de um hospedeiro, esperam o momento certo para o ataque e tentam se esconder para não serem exterminados.

O computador pode se infectar de diversas maneiras por disquetes, CDs, e-mails ou mesmo pelas páginas da internet. Alguns vírus podem apenas fazer brincadeiras no computador, outros podem até apagar

todos os dados em seu disco rígido. Eles estão agrupados em famílias com milhares de variantes.

1.18. DNS

O DNS (Sistema de Nomes de Domínios) é a maneira de localizar os nomes dos domínios na Internet e traduzi-los em endereços IP. Um nome de domínio é a representação fácil de ser lembrada de um endereço IP na Internet. A lista de nomes de domínios e endereços IP é um banco de dados distribuído e hierárquico.

Capítulo 3

ATAQUES REMOTOS

- Tipos de Ataque
- Mapeamento de Redes

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

Uma máquina remota é toda aquela que está distante da qual você está conectado atualmente e, pela rede local ou pela Internet, é possível de ser alcançada. Os riscos relacionados a um ataque remoto podem ser muito graves. Uma vez realmente conectado à sua máquina e com certos níveis de permissão, o hacker ou o cracker tem acesso à informações sigilosas, podendo apagar arquivos, desativar serviços, criar e excluir usuários. Por isso, todas as práticas recomendadas para proteção de ataques remotos devem ser tomadas. Os ataques remotos baseiam-se em informações conseguidas pelo hacker por meio da rede local ou da Internet. Certas informações são primordiais para estes tipos de ataque:

– Configuração da rede
– Fraquezas a serem exploradas
– Usuários pertencentes a esta rede
– Qual a origem da conectividade da rede

Essas informações podem ser obtidas por consultas remotas nos servidores que o hacker quer atacar. Vários utilitários podem ajudar com eficiência para conseguir informações como: a saída de conectividade desse servidor, o nome das máquinas conectadas, o sistema operacional instalado. É necessário descobrir o endereço do administrador,

essa informação terá um valor muito importante para poder executar alguns aplicativos do tipo *whois*, *nslookup* e *host*. Além disso, com essas informações é possível determinar a origem de conectividade do alvo, se é um nó folha ou domínio virtual.

As práticas recomendadas para firewall e as configurações de firewall padrão podem ajudar a proteger redes contra ataques remotos com origem externa ao perímetro da empresa. As práticas recomendadas sugerem bloquear todas as portas que não estejam sendo utilizadas no momento. Por essa razão, a maioria dos sistemas conectados à Internet deve ter um número mínimo de portas afetadas expostas.

1. Principais Modos de Operação

É difícil descrever um "modus-operandi" dos hackers durante uma invasão. Isto dependerá dos seus objetivos, da segurança existente, do sistema atacado etc. Um invasor terá que conseguir um acesso *shell* no sistema. Uma das coisas que um invasor tentará fazer, após entrar no sistema, é passar despercebido, apagando seus rastros dos arquivos de log e dos registros de usuários. Existem alguns programas prontos para isso, como o zap (e suas diversas versões), que alteram o arquivo utmp do UNIX. Com isso, comandos como o *who*, *w* e *finger* não mostram o invasor atuando. Ao mesmo tempo, os invasores tentarão esconder todos os arquivos e programas colocados no sistema, criando diretórios escondidos em áreas como o /tmp, /var/tmp/, /var/spool/mail. Depois, em muitos casos, os hackers tentarão obter privilégios de administrador do sistema (*root*, *sysadmin*, *manager*, *administrador*). Em sistemas UNIX, eles tendem a explorar vulnerabilidades conhecidas. Em servidores Windows, esse problema é ainda mais crítico, se o administrador não estiver antenado com as últimas atualizações de segurança (sevices packs), fatalmente terá sérios problemas de invasão remota.

Dentre as vulnerabilidades mais exploradas nos servidores Linux/UNIX, estão:

– Diversos problemas com rdist, sendmail, mail, lp, cron
– Variáveis de ambiente, em funções como popen()
– Race-conditions, em funções como access()
– Buffer overflow (em vários programas, como talkd, fingerd, elm)

– Criação de uma entrada inválida no passwd (usando o chfn)

Uma vez conseguindo esse privilégio, o invasor terá livre acesso a todos os recursos do sistema. Normalmente, os hackers tentarão substituir os seguintes programas do sistema:

– ps, ls, netstat, ifconfig e df (para esconderem sua presença e seus arquivos)
– telnetd e ftpd (para criarem entradas alternativas, caso sejam descobertos)
– login (para capturarem senhas de outros usuários)

Além de instalarem sniffers (para obter senhas de outros usuários em máquinas da mesma rede ou de fora, cujos pacotes passem pelo mesmo barramento), todos estes programas estão disponíveis nos chamados *rootkits*.

2. Análise do Ambiente-Alvo

Após definir o alvo e coletar algumas informações sobre o mesmo o hacker precisa fazer uma análise dos resultados obtidos, objetivando possíveis fraquezas no sistema do ambiente-alvo. Uma maneira de descobrir fraquezas de um sistema, UNIX, Linux ou Windows, é percorrer a Internet em busca dos boletins de falhas de segurança. Estes boletins são minas preciosas para hackers e crackers. Pois neles, podemos encontrar os detalhes das falhas de segurança dos sistemas operacionais, dos navegadores da Internet, dos bancos de dados, dos servidores Web, tais como: IIS, ColdFusion, ASP, PHP, JSP. Para identificar fraquezas de um sistema em questão, podemos utilizar ferramentas específicas para varrer o ambiente alvo, tais como ISS e Satan. O problema dessas ferramentas é que são muito perigosas, pois deixam rastros nos logs do sistema, então, sua eficácia é bastante discutível. Mas, se o ambiente-alvo possui um administrador relapso, essa é uma boa saída.

Os servidores DNS possuem, também, uma série de informações críticas sobre o sistema, então, vazamentos de informações sensíveis sobre a rede da organização ocorrem por transferências de zonas DNS. Essas informações podem ajudar um hacker a identificar os pontos fracos da rede e a escolher futuros alvos. Comprometimento do servidor

por vulnerabilidades no *software* de DNS, o que pode facilitar outras quebras de segurança no restante da rede da organização.

Funciona da seguinte maneira: o hacker descobre qual o ambiente, faz uma análise das possíveis brechas, busca por falhas conhecidas e, então, inicia seu ataque.

3. Mapeamento de Redes

O ICMP (*Internet Control Message Protocol*) é utilizado para ajudar na assistência do mapeamento de ambientes de rede. Com o propósito primário de transmitir mensagens de status e erros (ex.: host unreachable, redirect e time exceeded), ao invés da concepção de transportar dados, o protocolo pode ser utilizado por invasores para levantar informações do ambiente rede. A mais conhecida aplicação ICMP com certeza trata-se do *echo request* e *echo reply*. O ICMP *echo request* é um dos métodos mais utilizados para mapeamento de redes. O mapeamento da rede ajuda o hacker a obter informações muito importantes, tais como o número de servidores, o número de clientes, roteadores, switches, o tipo de sistema operacional, qual o firewall instalado. E também, em certos casos, descobrir números de IP válidos para esta rede. Com essas informações, o ataque torna-se mais fácil, pois assim o atacante pode definir onde deve atacar e com quais ferramentas. É de extrema importância restringir o echo request quando o mesmo é solicitado a partir da Internet com destino ao perímetro da rede. O famoso ataque de fragmentação "Ping of Death", utiliza pacotes icmp fragmentados para causar ataque do tipo Denial Of Service por meio da técnica de criar pacotes IP que excedem a especificação de 65,535 bytes de dados. Este ataque resulta, muitas vezes, em perda ou congelamento do host. Além do Ping of Death, um invasor pode obter informações preciosas pela análise das mensagens ICMP e utilizar o protocolo para a técnica de ataques do tipo *Smurf* ou *Loki*. Nesses casos, a recomendação é simplesmente o bloqueio de *incoming echo request* (*ping* e *Windows traceroute*) e bloqueio de *outgoing echo replies*, *time exceeded* (tempo excedido), e mensagens *unreachable* (inalcançáveis).

4. Ping

O PING (*Packet Internet Groper*) verifica se um endereço IP existe e está respondendo. Assim, a maioria dos hackers utilizam esse pequeno

programa para ver se existe o endereço descoberto, qual o seu tempo de resposta e qual a distância, dessa forma é um dos primeiros passos que o hacker toma. O uso mal intencionado desse programa, a partir de uma conexão rápida com a rede, faz com que a vítima caia num *lag* que provavelmente o levará a desconexão por Ping Timeout, devido a quantidade de pacotes recebidos superar em muito a sua capacidade de devolver os mesmos. O ping com pacotes acima de 1 Kb, eram chamados de Ping da morte ou "Ping of Death", pois ao "pingar" um host destino com este tamanho de pacote, a maquina saia do ar. Mas isso e classificado como um ataque do tipo *DoS*, e não invasão.

Capítulo 4

O PERIGO MORA AO LADO

- Engenharia Social
- Protegendo seus Dados

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

Nos preocupamos muito com a segurança externa de nossa rede, sempre nos protegemos de um possível ataque. Mas a maioria dos problemas de segurança são provenientes do próprio ambiente da empresa.

Este tipo de ataque ocorre geralmente por funcionários insatisfeitos, pessoas vingativas e invejosas, seu controle é dificultado porque, na maioria das vezes, os funcionários possuem informações que pessoas externas não têm acesso. Ataques físicos têm essa mesma origem, por falta de uma política de segurança interna, funcionários permitem acessos indevidos às suas máquinas, ou simplesmente fazem comentários que não deveriam.

1. Engenharia Social

Conversas informais podem gerar um grande volume de informações críticas, quando se está em um ambiente corporativo, podem representar a exposição total da empresa.

Engenharia Social é a aquisição de alguma informação ou privilégios de acesso inapropriado por alguém fora da empresa, baseando-se na construção de relações de confiança inapropriadas com as pessoas de dentro de uma organização. Ou seja, é a arte de manipular pessoas para conseguir alguma informação. O objetivo da Engenharia Social, como técnica de ataque, é enganar alguma pessoa para que ela diretamente

forneça informações, ou facilite o acesso a estas informações. Esta técnica é baseada nas qualidades da natureza humana, como a vontade de ajudar, a tendência em confiar nas pessoas e o medo de "se meter em problemas". São usadas como técnicas: perguntar datas de nascimentos; informações técnicas da rede, como número de máquina, tipos de equipamentos, sistemas operacionais instalados. Estas informações valiosas que expõem a empresa a ataques de hackers e crackers. Com uma combinação simples destes dados, é possível descobrir usuários, senhas, facilitando a ação desses criminosos virtuais.

2. Agenda

Toda e qualquer informação sigilosa deve ter um tratamento especial. Geralmente quando estamos em ambiente corporativo e trabalhamos com muitas pessoas, temos a tendência em confiar em todas elas por serem colegas de trabalho. Este é um paradigma a ser quebrado, pois não devemos confiar em pessoas que realmente não conhecemos. Por isto, deve-se ter muito cuidado com todo e qualquer objeto pessoal, tais como agendas, papéis importantes, carteiras, anotações importantes, tanto no papel quanto eletrônicos. Papéis jogados na lixeira também devem ser destruídos com cuidado, os hackers gostam muito de vasculhar lixeiras atrás de informações sigilosas. Se for jogar fora algum documento, verifique sempre se este foi inulizado. Os portáteis devem possuir sistemas de segurança para evitar livre acesso. São pequenas precauções que podem evitar grandes problemas de segurança. Não adianta uma empresa adquirir firewalls, sistemas de segurança para a rede e tudo mais, se os seus usuários (funcionários) não tiverem cuidado com as informações que possuem.

3. Arquivos

Os arquivos representam toda a produção intelectual do funcionário dentro da empresa, por isto, quase sempre são muito importantes e devem ser preservados muitas vezes, devem possuir acesso restrito. Assim, medidas simples podem ajudar evitar grandes problemas de roubo de idéias, segredos industriais ou intelectuais. Em redes Windows com compartilhamento de pastas, uma boa solução é compartilhar apenas uma pasta de cada máquina, esta pasta é usada para a transferência dos arquivos. Outra boa medida é utilizar senhas

nos arquivos mais importantes. Quase todos os aplicativos atuais possuem este recurso fácil de ser utilizado.

4. Hardware

Existem várias modalidades de ataques sorrateiros em nossos computadores pessoais e corporativos. Uma maneira clássica através de determinados itens de hardware que possuem vulnerabilidades, como: modems e gabinetes sem lacres de segurança. O modem é um dos maiores responsáveis por tráfico de informações não autorizadas para fora das empresas, pois se, em sua rede, os usuários locais podem fazer acesso discado à Internet, então, não se tem controle do que está entrando e saindo dos limites corporativos. Outra coisa importante é a quantidade de portas abertas que os modems possuem, como geralmente não passam por um firewall, uma conexão discada direta é um risco iminente. Então, a melhor opção é sempre retirar todos os modems dos usuários locais, e deixar somente o modem que é o gateway para Internet.

Geralmente, a segurança da máquina é deixada de lado na maioria das empresas, um gabinete sem lacres de segurança pode ser invadido. Um funcionário mal-intencionado facilmente retirar discos rígidos do gabinete, pode inserir um novo disco rígido e copiar dados importantes. A melhor opção é adotar medidas de segurança, tais como lacres rígidos para os gabinetes e monitoração por filmagens.

5. E-mail

Na Internet, o e-mail é um dos serviços mais usados, pois traz várias facilidades de transmissão de documentos a baixíssimo custo. Entretanto, os e-mails são muito vulneráveis quanto à segurança de conteúdo e autenticação pessoal de envio. Isso quer dizer que os dados que nele trafegam podem ser captados e lidos com muita facilidade, assim como pode haver falsidade ideológica em relação ao envio do e-mail, basta ter acesso ao endereço do e-mail de alguma pessoa para enviar alguma mensagem em seu nome. Ferramentas de criptografia e autenticação estão sendo usadas hoje em dia para prevenir estes tipos de problemas, como o OpenPGP (Prety Good Privacy) e S/MIME.

Os e-mails são transmitidos sem conexão direta entre o emissor e o destinatário da mensagem, sendo assim, não é possível criar algum

tipo de canal de comunicação segura, como pode ser feito nos casos de protocolos como o HTTP e o SSL. A transmissão para o servidor é feita pelo protocolo SMTP, que funciona no modelo "store-and-forward", o qual envia a mensagem para o servidor do e-mail de origem, este se encarrega de passar para os servidores de destino, onde ficam gravados até que seja feito o download pelos destinatários. Neste método, está o principal problema com a segurança de e-mails, porque, enquanto estão no servidor, os e-mails podem sofrer algum tipo de violação.

Outro grande problema com o envio de e-mail é que se torna uma forte via de distribuição de vírus. Isto ocorre devido a arquivos anexados, os quais às vezes trazem vírus que podem danificar o computador e se auto-enviar para todos os e-mails cadastrados na lista de contatos do cliente (Outlook, Eudora etc.). A solução é sempre possuir um antivírus atualizado na máquina local e também um servidor de e-mail com verificação de vírus.

A utilização programa responsável de receber os e-mails merece também um destaque. Na maioria das vezes os usuários configuram seus programas para recebimento automático dos e-mails, deixando o endereço de e-mail e senhas salvos. Isso é muito sério, pois assim qualquer pessoa que venha a utilizar essa máquina terá acesso a todos os e-mails já recebidos e também poderá receber os novos. Duas maneiras práticas de resolver isso, primeiro, criar perfis de usuários no gerenciador de e-mails protegidos por senha e, segundo, nunca salvar sua senha para receber e-mails automaticamente.

6. Cookies

Os cookies são arquivos texto (.txt) enviados pelo servidor web para os browsers que visitam suas páginas. Estes arquivos são armazenados localmente na máquina do usuário e são ativados toda a vez que a página que os gerou é acessada. Pelos cookies, os programadores web podem gravar qualquer informação que o usuário tenha informado via browser.

Os cookies servem para informar aos servidores web quantas vezes uma mesma página é acessada pelo mesmo browser, podem servir também para ativar páginas customizadas para um usuário. Mas além das boas intenções, os cookies podem nos trazer dores de cabeça, por exemplo, se alguém os roubar de sua máquina e neles estiverem infor-

mações críticas, por programas simples de descriptografia, o hacker pode acessar essas informações e usá-las indevidamente.

Os problemas maiores são as falhas de segurança dos navegadores, se procuramos verdadeiramente segurança, podemos adotar algumas maneiras para evitar os cookies. Uma idéia é desativar sua utilização do *navegador em uso e sempre verificar a confiabilidade e a integridade do* site que estamos enviando dados. Outra tática é apagar regularmente o conteúdo da pasta de cookies da máquina.

7. Internet

O acesso indiscriminado à Internet é um problema enfrentado por quase todas as empresas. Por vários motivos, um deles é perda de tempo, pois os funcionários ao invés de trabalharem em prol de suas atribuições ficam dispersos, navegando indiscriminadamente pela Web. Outro problema é o conteúdo dos sites visitados, muitas vezes os usuários enveredam por sites com conteúdos maliciosos e colocam em risco a segurança da empresa. Outro fator é a performance. Às vezes, um usuário local pode carregar a banda da rede, fazendo download de vídeos ou imagens pornográficas. Atualmente, existem várias maneiras de solucionar estes problemas, como: criação de políticas de segurança de acesso à Internet; instalação de softwares que monitoram e bloqueiam acesso indevido; autenticação de usuário na rede, propiciando assim total controle de cada passo do cliente.

Mas talvez o problema mais sério e mais difícil de ser remediado seja realmente a saída de informações dos limites da empresa. A maioria das empresas não possui monitoração de informações que saem por e-mail. A solução nestes casos é definir quais os critérios de segurança serão adotados e então usar algumas das ferramentas disponíveis no mercado, como por exemplo, controles de segurança no IIS da Microsoft, no caso de servidores Windows; sendmail, no caso de servidores Linux, entre outros programas, ou mesmo softwares específicos que filtram e controlam o tráfego de e-mails nas empresas.

8. Backup

Ameaças de vírus, ataques ou qualquer outra atividade maliciosa influenciam diretamente, na operação de uma empresa, desde um usuário local até uma rede corporativa.

Quando acontece alguma falha de segurança ou desastre, ao invés de perseguir a origem, o foco principal é restaurar os recursos de tecnologia da informação para sua total funcionalidade. Quanto maior for a demora, maiores serão as conseqüências para a empresa. Backups diários ou semanais dos sistemas, incluindo dados essenciais para operação da empresa, são componentes vitais para restauração de desastres.

Apesar de ser uma medida de segurança antiga, muitas empresas não possuem um sistema de backup ou o fazem de maneira incorreta. Comumente, o backup é feito sem criptografia e armazenado no mesmo local do servidor principal da corporação. Assim, qualquer pessoa que tenha acesso a este local (sala, armário sem chaves) poderá ter acesso à estes dados. CDs gravados como backup, com nomes sugestivos, podem ser um grave problema. Pois, o hacker pode simplesmente pegar o CD já sabendo o seu conteúdo e copiá-lo. O ideal é armazenar os backups em locais seguros, onde haja um acesso restrito de pessoas. Também é aconselhável fazer backups com algum tipo de criptografia e gerar logs dos acessos aos backups.

Capítulo 5

TROJANS

• Definição de Trojans

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

O termo vem da *Ilíada*, de Homero, em que os gregos dão um cavalo de madeira a seus inimigos troianos, como uma oferenda de paz. Depois que os troianos levam o "presente" para dentro da cidade, soldados gregos saem de dentro do cavalo e abrem os portões para seus compatriotas, permitindo-lhes capturar e dominar Tróia. A história também gerou o conceito do "presente de grego", definição que se encaixa à perfeição nos trojans da era digital.

Não devemos confundi-los com um vírus, pois o vírus é um programa autônomo programado para se auto-reproduzir. Claro, além de suas outras funções, como apagar ou comprimir arquivos, o trojan sozinho não faz nada. Ele vem com poucos comandos automáticos como estes:

- Auto-reproduzir.
- Editar os arquivos de inicialização e registro do Windows.
- Abrir uma porta.
- Enviar um e-mail ou mensagem para instant messengers (ICQ, MSN Messenger, Yahoo etc.) direto para o invasor, avisando-o quando você estiver on-line.

Quando o trojan é configurado, o invasor tem quase controle total da máquina da vítima, pode até mesmo formatar o HD, mover o mouse,

capturar tela, acessar qualquer arquivo até mesmo abrir o drive de CD-ROM.

Sempre que pensar em trojan, lembre-se: ele é **um interpretador de comandos remoto.**

Um perigo real

Os fatores que fazem deste método de invasão um dos mais perigosos da atualidade são:

– O crescimento da Internet.
– A grande gama de programas trojans disponíveis.
– O Trojan não utli falhas dos Sistemas Operacionais.
– A simplicidade de alguns programas.

Hoje em dia, uma pessoa com pouco conhecimento de informática pode facilmente usar um trojan. É possível esconder um trojan em fotos, arquivos compactados, e-mails, arquivos de música, aplicativos e jogos. Com isso, não devemos executar arquivos que não tenham uma procedência confiável e nunca se esquecer de atualizar o antivírus.

Existem muitos programas na Internet que escondem os servidores em arquivos executáveis. Um deles é o *The Joiner*, que possibilita juntar o trojan com algum outro executável e, assim, criar um terceiro arquivo contendo os dois. Além de possibilitar que o coloque em fotos. Um método engraçado muito utilizado hoje pelos que se dizem "hackers" é renomear algum executável para foto e deixar um largo espaço. Por exemplo: Supondo que o nosso servidor é o arquivo ***server.exe***, então, iríamos renomeá-lo para loira.jpg   .exe.

Assim, muitos usuários inexperientes caem no truque. Todos os métodos citados anteriormente têm somente uma falha: se você criar um executável pelo *The Joiner* ou renomear o servidor, qualquer programa antivírus logo detectará o arquivo. Para que o antivírus não o detecte, é só usar a imaginação. O hacker cria um programa em alguma linguagem e coloqua o servidor no meio dos arquivos. Fazendo com que o programa, quando executado, renomeie o servidor e o execute. Assim, se o servidor estiver como *voodoo.dll*, passe-o para *sysconf.exe* e execute. Esse método não é infalível, mas engana a maioria dos programas de detecção. Claro, se você utilizar um bom antivírus, ele geralmente o detecta o trojan.

Tipos de cavalo de tróia (TROJAN)

Invasão por portas TCP e UDP

Netbus, *Back Orifice*, *SubSeven*, *Hack'a'tack*, *Girlfriend* e *Netsphere* são os trojans mais usados e propagados na Internet atualmente e são facilmente encontrados pela rede. Possuem, em sua maioria, dois arquivos: um servidor para ser instalado no computador da vítima e um cliente, com interface gráfica, para manipular o servidor remotamente.

As portas de um sistema variam entre 0 e 65535 e servem para identificar serviços rodando no sistema (como o servidor web que utiliza a porta 80). O servidor se torna mais um serviço ao escolher alguma porta para "escutar" as chamadas do cliente. O trojan que utiliza portas TCP estabelece uma conexão com o servidor na porta definida pelo hacker na maioria dos casos, atuando diretamente dentro do sistema. Já o trojan que utiliza portas UDP comunica-se via pacotes de dados enviados ao host alvo, no caso o computador onde está instalado o server. Não tão confiável como o TCP, não garante a entrega dos pacotes e o recebimento da resposta. Quase todos os trojans atuais são para a arquitetura Windows. Os poucos existentes em outros sistemas, tais como: Unix, Linux, Novell e Macintosh são chamados de *backdoors*. A diferença entre o trojan comum e o backdoor é que o último é muito mais difícil de ser instalado, pois, para instalar o server em sistemas UNIX, é necessário estar logado como superusuário (root).

Trojans de informação

Não é tão usado quanto o de portas, mas é mais perigoso. Enquanto a maioria das funções dos trojans comuns é apenas para aborrecer (sumir com a barra de tarefas, apagar o monitor, desligar o Windows etc.), o trojan de informação se concentra em ficar residente, detectando todos os tipos de dados vitais do sistema. Ele consegue toda senha digitada no servidor junto ao endereço ip das máquinas e envia a informação para uma conta de e-mail configurada pelo invasor. Existem alguns programas mais sofisticados que, além de avisar por e-mail, podem enviar a informação por *icq* ou qualquer outro tipo de instant messenger. Geralmente, o programa envia a informação em um prazo de 5 a 10 minutos configurado pelo usuário. Ao contrário do trojan de portas que

possui apenas o arquivo servidor e um tamanho bem menor. Exemplo: O servidor do trojan de portas Netbus tem cerca de 490 kb, já o trojan de informações k2ps possui cerca de 17 kb.

Trojans de ponte

É um tipo não muito conhecido, mas bem usado por hackers e crackers. Consiste em instalar um servidor no seu computador que possibilite ao invasor realizar ataques de invasão e de recusa de serviço. Então, se um grande site for invadido e baterem em sua casa, procure, pois deve haver algum desses trojans de ponte no seu sistema. Um programa comum é o WinProxy, que pode ser instalado facilmente e não levanta nenhum tipo de suspeita.

Trojans comerciais

Já ouviu falar do PcAnywhere? Ou do terminal remoto do Windows 2000 e XP? Esses programas, além de muitos outros, possibilitam que você controle remotamente a máquina de cliente como se estivesse sentado nela. A vantagem desses programas para os hackers, já que são comerciais, é que os antivírus não os detectam. Um dos mais usados no mercado é o VNC (http://www.download.com, gratuitamente). Se configurar corretamente um desses programas, é possível acesso completo à máquina, podendo desde copiar um arquivo até formatar o disco.

Portas usadas por trojans

Esta tabela mostra as portas mais utilizadas pelos trojans existentes atualmente.

Nome do Trojan	Portas Usadas	Protocolo
2000 Cracks	6776	TCP
Acid Battery	32418	TCP
Acid Battery 2000	52317	TCP
Acid Shivers	10520	TCP
Agent 31	31	TCP
Agent 40421	40421	TCP
Aim Spy	777	TCP
Ajan	25	TCP
Ambush	10666	UDP

AntiGen	25	TCP
AOL Trojan	30029	TCP
Attack FTP	666	TCP
Back Construction	666/5400/5401	TCP
Back Door Setup	5000/5001/7789	TCP
Back Orifice	31337/31338	UDP
Back Orifice 2000	8787/54320/54321	TCP
Back Orifice DLL	1349	UDP
BackDoor	1999	TCP
BackDoor-G	1243/6776	TCP
BackDoor-QE	10452	TCP
BackDoor-QO	3332	TCP
BackDoor-QR	12973/12975	TCP
BackFire	31337	UDP
Baron Night	31337	TCP
Big Gluck (TN)	34324	TCP
BioNet	12349	TCP
Bla	1042/20331	TCP
Black Construction	21	TCP
Blade Runner	21/5400-5402	TCP
BO Client	31337	TCP
BO Facil	5556/5557/31337	TCP
BO Wack	31336	TCP
BoBo	4321	TCP
BOWhack	31666	TCP
BrainSpy	10101	TCP
Bubbel	5000	TCP
BugBear	36794	TCP
Bugs	2115	TCP
Bunker-Hill	61348/61603/63485	TCP
Cain e Abel	666	TCP
Chargen	9	UDP
Chupacabra	20203	TCP

Coma	10607	TCP
Cyber Attacker	9876	TCP
Dark Shadow	911	TCP
Death	2	TCP
Deep Back Orifice	31338	UDP
Deep Throat	41/2140/3150/6771	TCP
Deep Throat v2	2140/3150/6670/6711/ 60000	TCP
Deep Throat v3	6674	TCP
DeepBO	31337	UDP
DeepThroat	999	TCP
Delta Source	26274	UDP
Delta Source	47262	UDP
Der Spacher 3	1000/1001/2000/2001	TCP
Devil	65000	TCP
Digital RootBeer	2600	TCP
DMsetup	58/59	TCP
DNS	53	TCP
Doly Trojan	21/1010-1012/1015	TCP
Donald Dick	23476/23477	TCP
DRAT	48/50	TCP
DUN Control	12623	UDP
Eclipse 2000	3459	TCP
Eclypse	3801	UDP
Email Password Sender	25	TCP
Evil FTP	23456	TCP
Executer	80	TCP
File Nail	4567	TCP
Firehotcker	79/5321	TCP
Fore	21/50766	TCP
FTP - Trojan	21	TCP
FTP99cmp	1492	TCP
Gaban Bus	12345/12346	TCP

Gate Crasher	6969/6970	TCP
GirlFriend	21554	TCP
Gjamer	12076	TCP
Hack '99 KeyLogger	12223	TCP
Hack 'a' Tack	31780/31785/31787-31789	TCP
Hack 'a' Tack	31791/31792	UDP
HackCity Ripper Pro	2023	TCP
Hackers Paradise	31/456	TCP
HackOffice	8897	TCP
Haebu Coceda	25	TCP
Happy 99	25/119	TCP
Hidden Port	99	TCP
Hooker	80	TCP
Host Control	6669/11050	TCP
HVL Rat5	2283	TCP
icKiller	7789	TCP
ICQ (www.mirabilis.com)	1027/1029/1032	TCP
ICQ Revenge	16772/19864	TCP
ICQ Trojan	4590	TCP
Illusion Mailer	2155/5512	TCP
InCommand	9400	TCP
Indoctrination	6939	TCP
Infector	146	TCP
Infector	146	UDP
INi-Killer	555/9989	TCP
Insane Network	2000	TCP
Invisible FTP	21	TCP
IRC-3	6969	TCP
JammerKillah	121	TCP
Kazimas	113/7000	TCP
Kuang2	25/17300/30999	TCP
Larva	21	TCP

Logged	20203	TCP
Masters' Paradise	31/3129/40421-40423/ 40425-40426	TCP
Mavericks Matrix	1269	TCP
Millenium	20000-20001	TCP
MiniCommand	1050	TCP
Mosucker	16484	TCP
Nephron	17777	TCP
Net Administrator	21/555	TCP
Net Controller	123	TCP
Netbios Datagram (DoS Attack)	138	TCP
Netbios Name (DoS Attack)	137	TCP
Netbios Session (DoS Attack)	139	TCP
NetBus	12345-12346	TCP
NetBus Pro	20034	TCP
NetMetropolitan	5031	TCP
NetMonitor	7300-7301/7306-7308	TCP
NetRaider	57341	TCP
NETrojan	1313	TCP
NetSphere	30100-30103	TCP
NetSpy	1024/1033/31338-31339	TCP
NewApt	25	TCP
NoBackO	1200-1201	UDP
One of the Last Trojan (OOTLT)	5011	TCP
OpC BO	1969	TCP
PC Crasher	5637-5638	TCP
Phase Zero	555	TCP
Phineas Phucker	2801	TCP
Pie Bill Gates	12345	TCP
Portal of Doom	3700/9872-9875	TCP
Portal of Doom	10067/10167	UDP

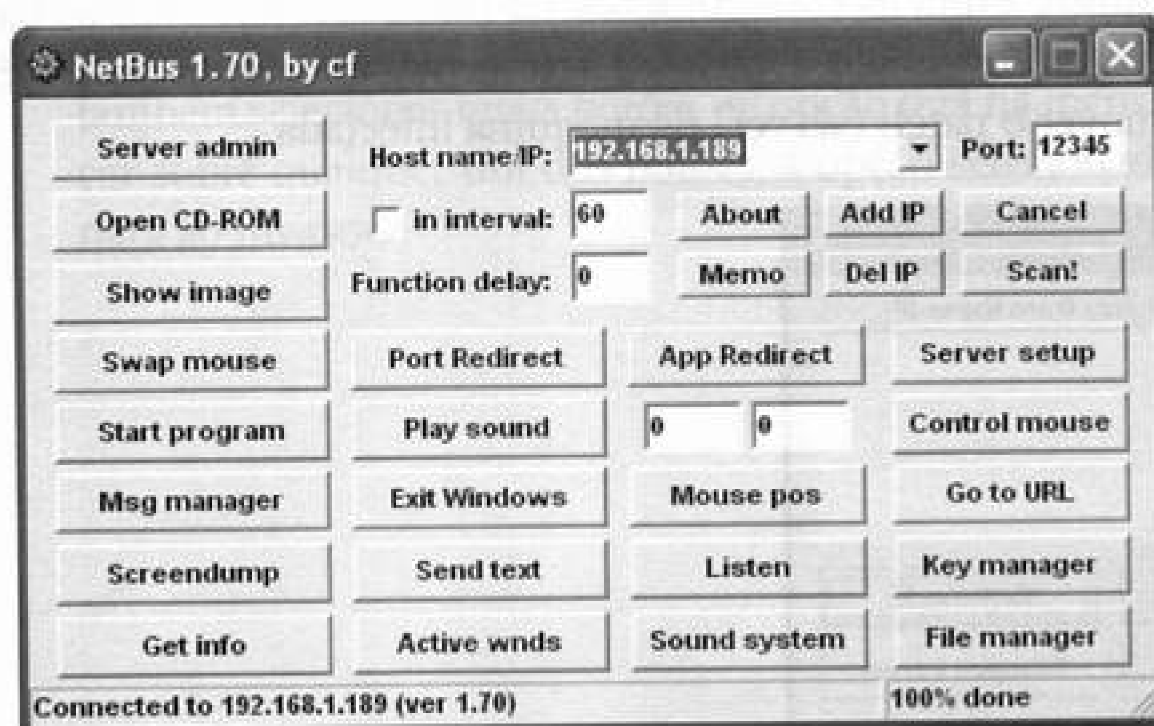
Priority	6969/16969	TCP
Progenic	11223	TCP
ProMail Trojan	25/110	TCP
Prosiak	22222/33333	TCP
Psyber Stream Server	1024/1170/1509/4000	TCP
Rasmin	531/1045	TCP
RAT	1095/1097-1099/2989	TCP
RC	65535	TCP
Rcon	8989	TCP
Remote Grab	7000	TCP
Remote Windows Shutdown	53001	TCP
RingZero	80/3128/8080	TCP
Robo-Hack	5569	TCP
Satanz BackDoor	666	TCP
ScheduleAgent	6667	TCP
School Bus	54321	TCP
Schwindler	21554/50766	TCP
Secret Agent	11223	TCP
Secret Service	605/6272	TCP
Senna Spy FTP Server	21/11000/13000	TCP
ServeMe	5555	TCP
ServeU	666	TCP
Shadow Phyre	666	TCP
Shit Heep	6912	TCP
ShockRave	1981	TCP
Shtirlitz	25	TCP
Sivka-Burka	1600	TCP
SK Silencer	1001	TCP
Socket25	30303	TCP
Sockets de Troie	5000-5001/30303/50505	TCP
SoftWAR	1207	TCP
Spirit 2001a	33911	TCP

SpySender	1807	TCP
Stealth	25	TCP
Stealth Spy	555	TCP
Streaming Audio Trojan	1170	TCP
Striker	2565	TCP
SubSeven	1243/2773/6711-6713/6776/7000/7215/27374/27573/54283	TCP
SubSeven Apocalypse	1243	TCP
Syphillis	10086	TCP
Tapiras	25	TCP
TCP Wrappers	421	TCP
TeleCommando	61466	TCP
Terminator	25	TCP
Terror Trojan	3456	TCP
The Invasor	2140/3150	TCP
The Prayer	2716/9999	TCP
The Spy	40412	TCP
The Thing	6000/6400	TCP
The Traitor	65432	TCP
The Traitor	65432	UDP
The Trojan Cow	2001	TCP
The Unexplained	29891	UDP
Tiny Telnet Server	23/34324	TCP
TransScout	1999-2005/9878	TCP
Trinoo	34555/35555	UDP
Truva Atl	23	TCP
Ugly FTP	23456	TCP
Ultor's Trojan	1234	TCP
Vampire	1020	TCP
Vampyre	6669	TCP
Virtual Hacking Machine	4242	TCP
Voice	1024/1170/4000	TCP

Voodoo Doll	1245	TCP
Wack-A-Mole	12361-12362	TCP
Web Ex	21/1001	TCP
WhackJob	12631/23456	TCP
WinCrash	21/2583/3024/4092/ 5714/5741-5742	TCP
WinGate (Socks-Proxy)	1080	TCP
WinHole	1080/1082	TCP
WinNuke	135/139	TCP
WinPC	25	TCP
WinSatan	999	TCP
WinSpy	25	TCP
X-Bill	12345-12346	TCP
Xplorer	2300	TCP
Xtcp	5550	TCP
Xtreme	1090	TCP
YAT	37651	TCP

NETBUS 1.7

O NetBus é um dos trojans mais utilizados atualmente, todas as ações são feitas a partir de uma tela principal. Veja seus principais comandos:



Host name/IP: Coloque o IP da máquina em que você instalou o server foi instalado.

Port: Porta configurada no patch.exe (server, a porta padrão é 12345).

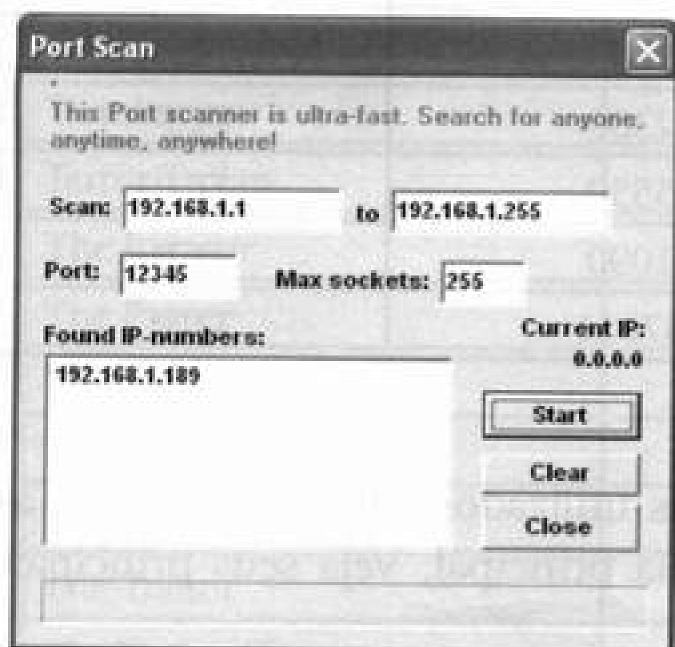
In interval, Function delay, Memo e About: Deixe como está.

Add IP: Caso o IP (HOST) seja fixo, deve ser adicionado na lista.

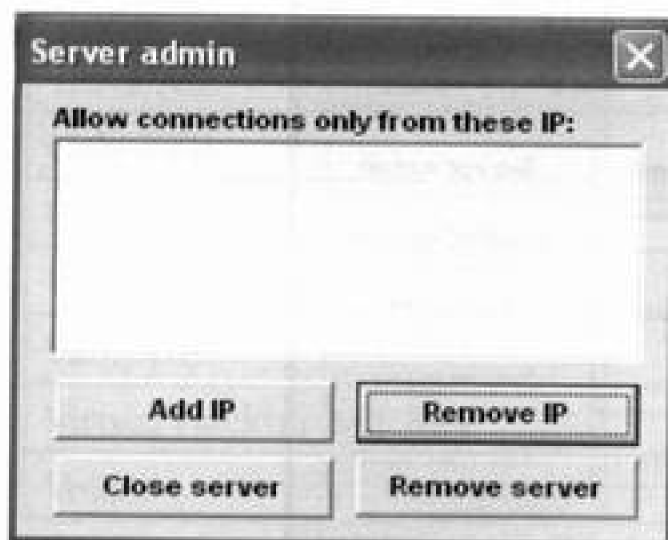
Del IP: Deletar o IP colocado anteriormente na lista.

Connect: Após colocar o IP (HOST) e a porta, deve clicar em *connect* para conectar.

Scan: Escaneia IPs infectados com o patch (server). No caso abaixo, ele vai escanear do ip 192.168.1.1 até 192.168.1.255 na porta 12345. Na janela found IP-numbers, ele mostra quais os ips (hosts) infectados nesta faixa que vai de 1 a 255 com o patch (server).

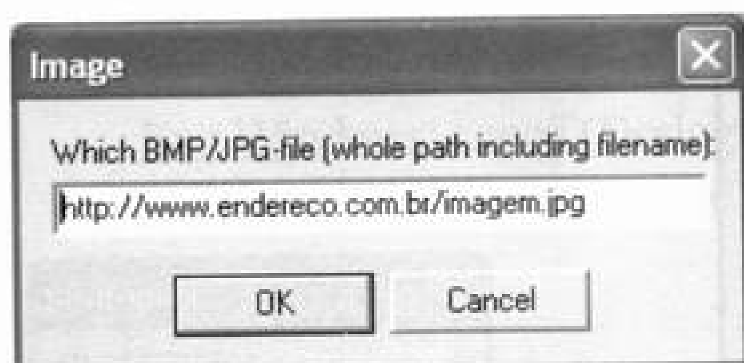


Server Admin: Edita as configurações do patch (server) NetBus da máquina na qual conectado. É possível acrescentar e remover ips e, até mesmo, remover o patch (server) da máquina infectada.



Open CD-ROM: Esta opção faz o CD-ROM abrir e fechar alternando conforme este botão é clicado.

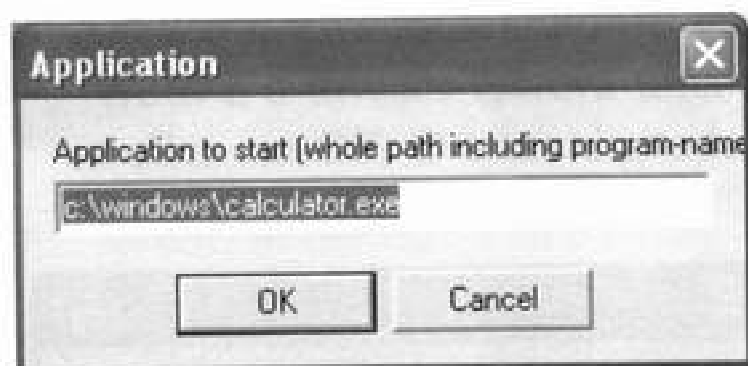
Show image: Digitando uma URL de uma foto, por exemplo, http://www.endereco.com.br/imagem.jpg , a imagem aparecerá em uma janela da máquina em que está instalado o patch (server).



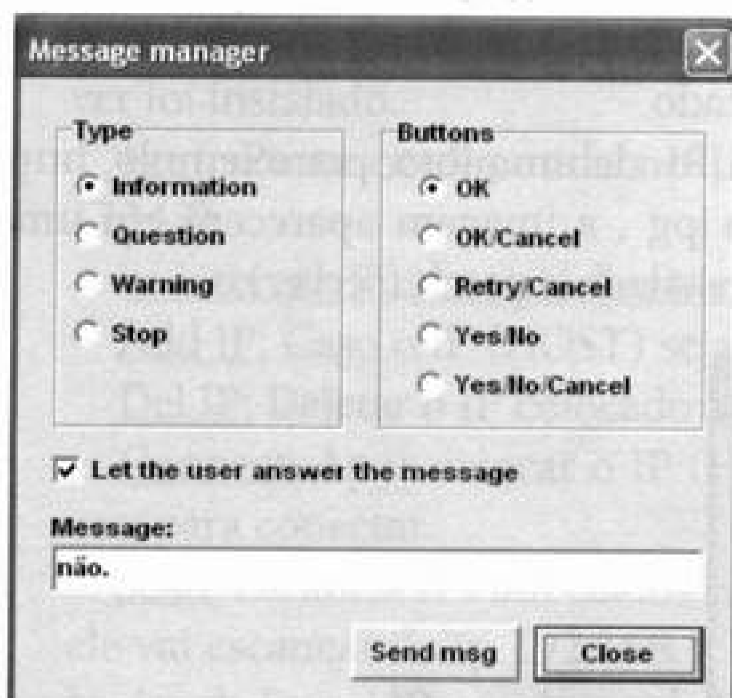
Swap Mouse: Inverte os botões do mouse.

Start Program: Executa um programa no micro em que está instalado o patch (server).

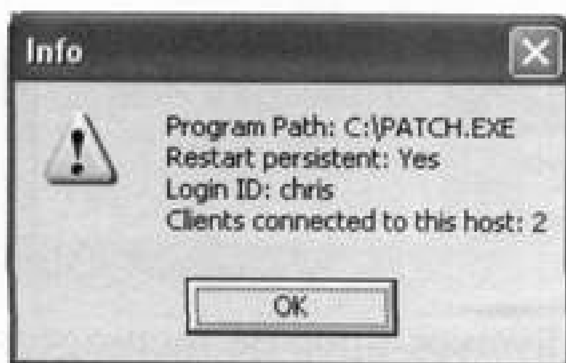
Ex.: c:\windows\calc.exe



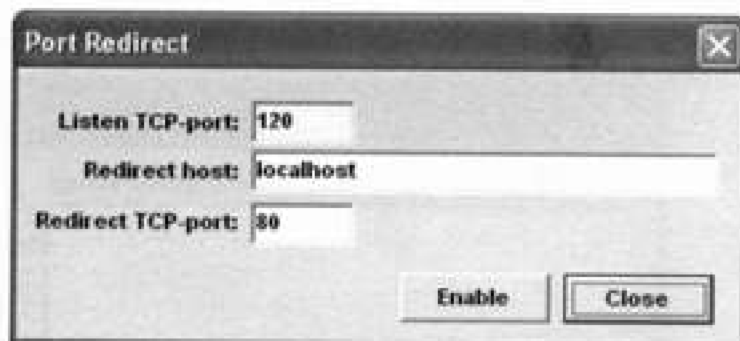
Msg Manager: Possibilita o envio de diversos tipos de mensagens usadas pelo sistema da vítima. Se você marcar o botão *Let the user answer the message*, a vitima poderá responder a mensagem. Pode-se também selecionar quais botões de opção terá na mensagem. Após clicar sobre qualquer um dos botões, a opção selecionada por ela retornará ao invasor.



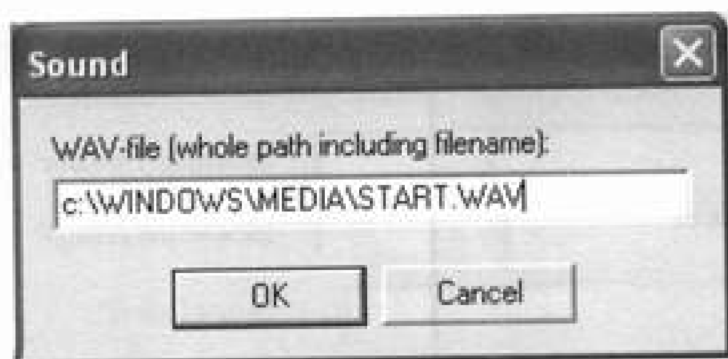
Screendump: Faz um PrintScreen na tela da vítima, salvando a imagem no diretório do netbus com o nome de temp1.bmp. Get Info: Informa qual cliente está sendo usado para a conexão, se a conexão é persistente, nome da máquina e quantos clientes estão conectados no patch (server).



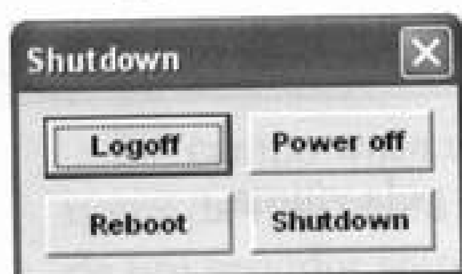
Port Redirect: Redireciona as portas.



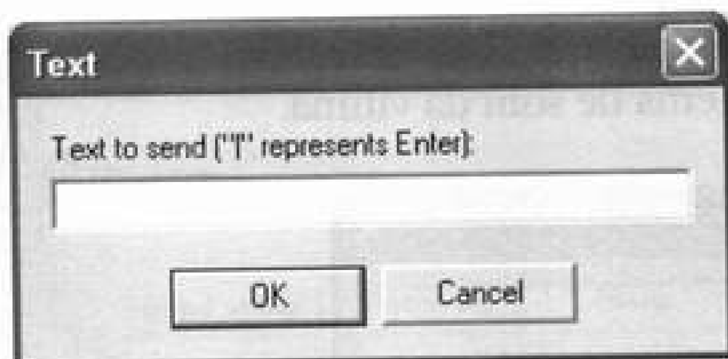
Play Sound: Toca um som no formato wav, que está presente no micro da vítima. É só colocar o caminho para o arquivo no campo texto e clique em OK.



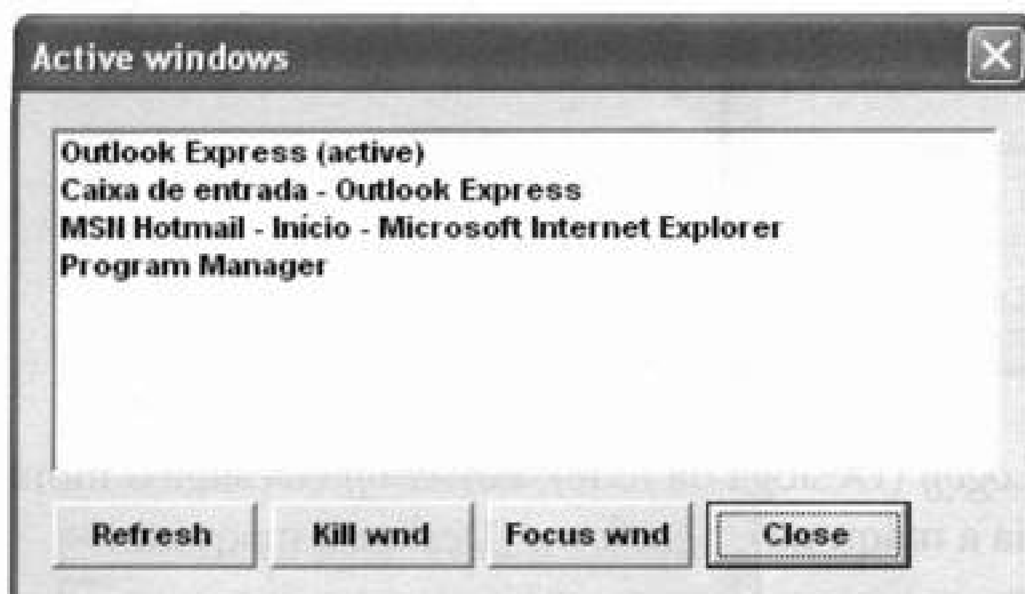
Exit Windows: *Logoff* (Desloga da rede), *Power off* (Desliga o monitor), *Reboot* (reinicia a máquina), *Shutdown* (Desliga a máquina).



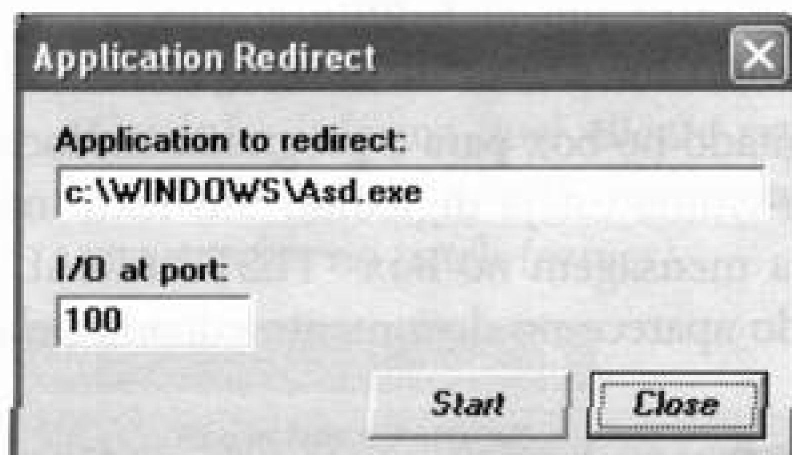
Send Text: Envia o texto digitado no box para o programa em foco no momento. Suponha que a vítima esteja digitando um texto no Word e o invasor escreva uma mensagem no Box "TESTE FINAL" e clica em OK. O texto digitado aparece no documento editado pela vítima no momento.



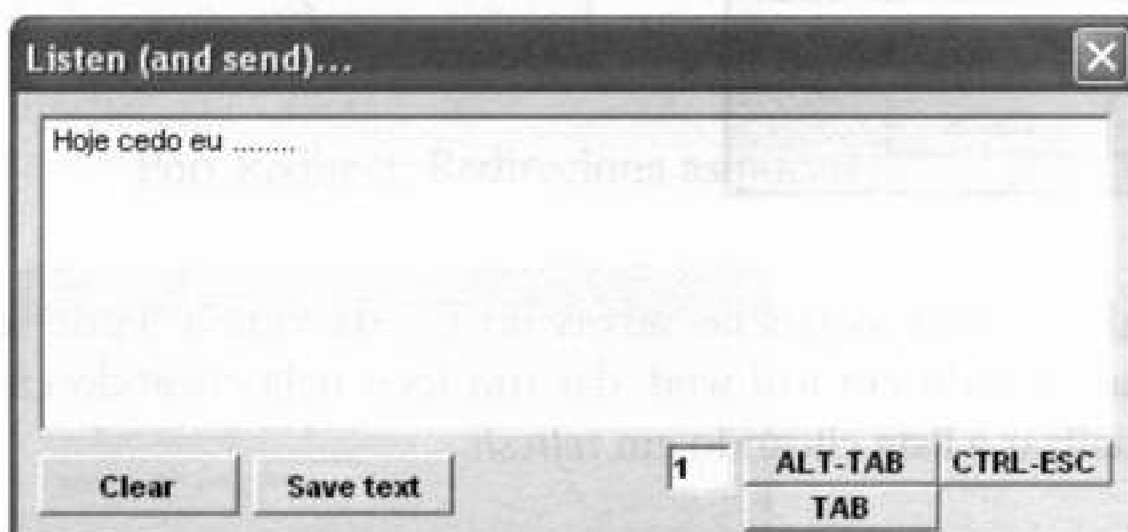
Active Wnds: Mostra as janelas ativas no PC da vítima, Pode-se fechar a janela clicando em *Kill wnd*, dar um foco nela clicando em *Focus wnd*, atualizar a lista clicando em *refresh*.



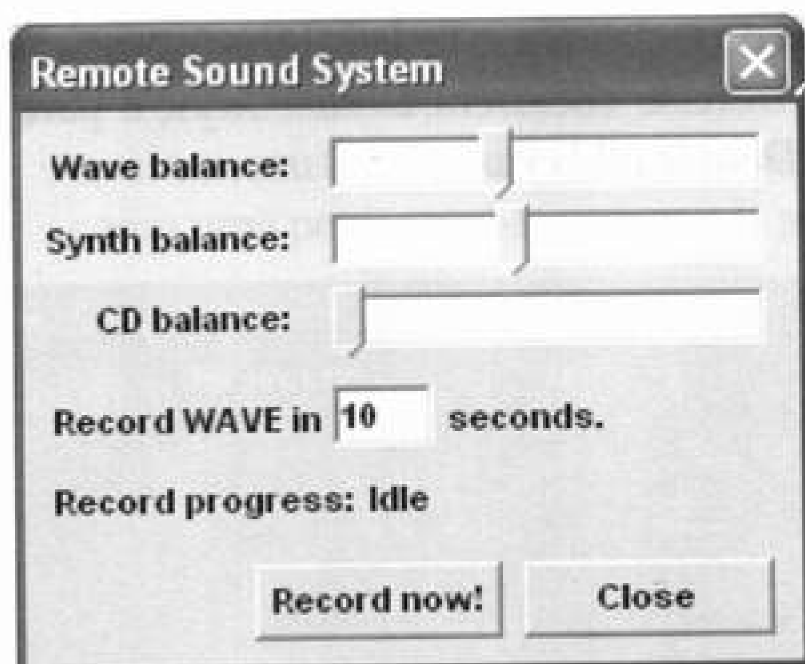
App Redirect: Redireciona a aplicação.
Mouse Pos: Define a posição para o mouse.
Listen: Captura todas as teclas pressionadas pela vítima.



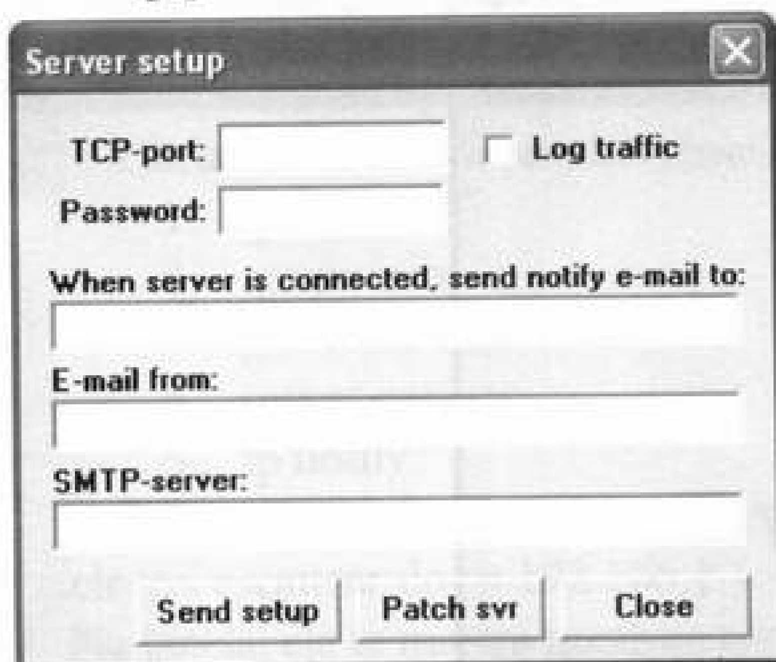
Sound System: Controla o sistema de som da vítima.



Server Setup: Muda as configurações do patch (server) instalado na máquina da vítima. Pode-se colocar senha para que somente o invasor acesse esse host, para colocar senha, basta preencher o campo password. Para que o invasor seja notificado quando a vítima estiver on-line, tem de preencher os outros campos.

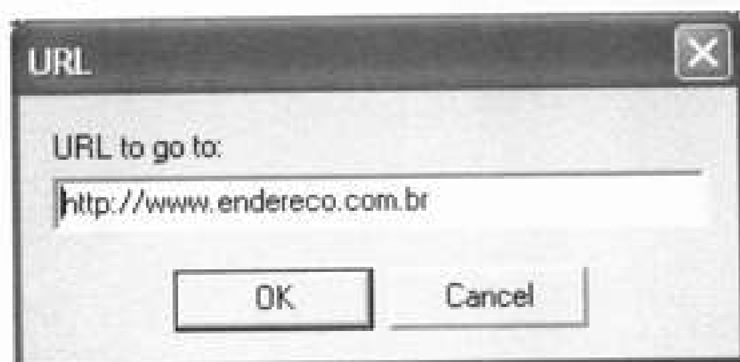


No campo *when server is connected, send notify e-mail to,* coloque o nome da vítima; em *E-mail from*, a e-mail, em *SMTP-server,* o endereço de um servidor smtp. Preenchidos todos os campos, clica-se em *Send setup* para salvar as alterações.



Control Mouse: Controla o mouse da vítima, você mexe o dela com o seu. Para parar de controlar, aperte o botão novamente.

Go to URL: Coloque o endereço no box e clique em *ok*. O navegador padrão da vítima abre com o endereço digitado no box.



Key Manager: Desativa teclas do teclado ou o teclado da pessoa. Para desabilitar só algumas teclas, deve-se clicar em *Disable keys*; e para desabilitar todo o teclado, em *Disable all keys*.

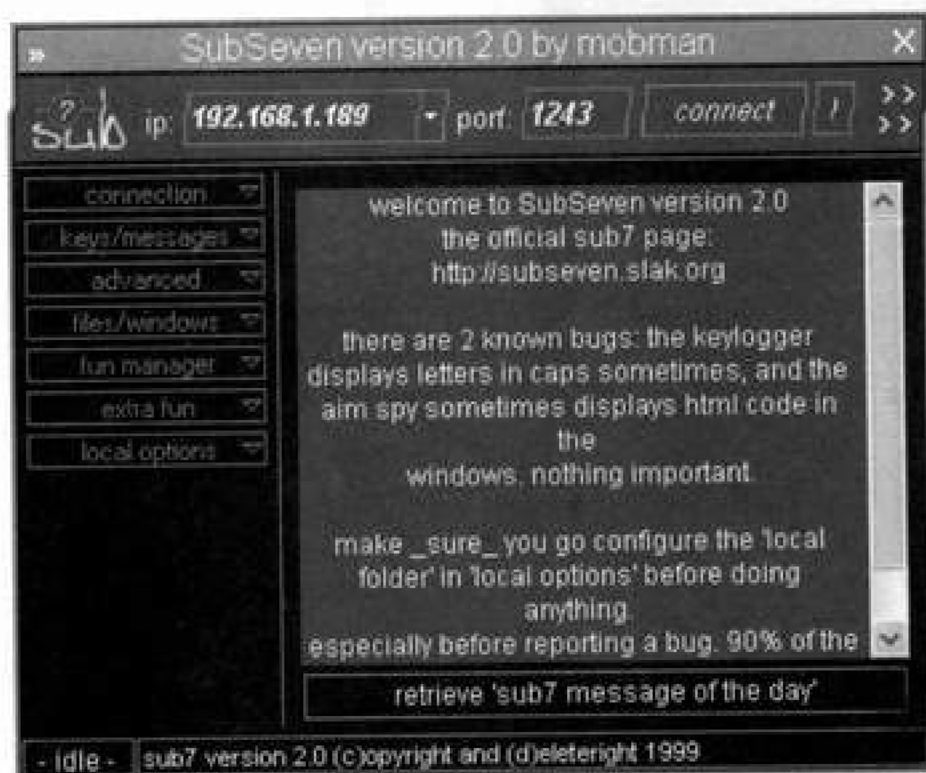


File Manager: Acesso total aos arquivos e às partições da vítima. Você pode colocar, remover e copiar arquivos.



SubSeven 2.0

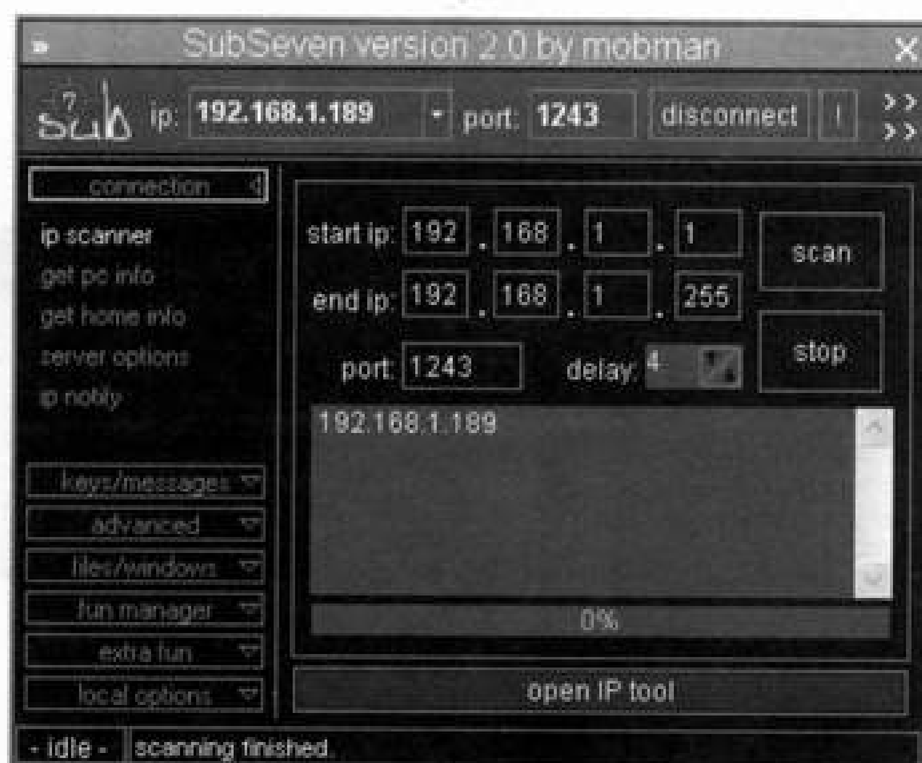
Como o NetBus, o SubSeven é um trojan muito utilizado por hackers/ crackers, seu funcionamento é bem parecido como NetBus. Veja a seguir como uma pessoa mal-intencionada acessa outras máquinas.



Clicando na aba *connection* temos:

1. ip scanner
2. get pc info
3. get home info
4. server options
5. ip notify

1. Ip scanner: Escaneia IPs infectados com o server. No caso abaixo, ele vai escanear do ip 192.168.1.1 até 192.168.1.255, na porta 1243. Na janela, ele te mostra quais os ips (hosts) infectados nesta faixa que vai de 1 a 255. Para iniciar, clique em *scan*; para parar, em *stop*.



Clicando em *open IP tool*, é apresentada uma ferramenta de resolução de nomes. Para saber o ip de determinado site, basta colocar o endereço no campo *host name* e clicar no botão *resolvem host name*. O resultado será o similar do apresentado abaixo.



2. Get pc info: Retorna informações referentes à máquina da vítima.
Computer name = Nome da máquina na rede.
User name = Nome do usuário que está usando o sistema.
Windows folder = Pasta onde o windows foi instalado.
System folder = Pasta do system.
Computer owner = Para quem está registrado o windows.
Company = Nome da empresa que o windows está registrado.
Version = Versão do sistema.

Platform = Plataforma usada (Windows 95, 98, Me, Xp etc.).

Resolution = Qual a configuração da máquina.

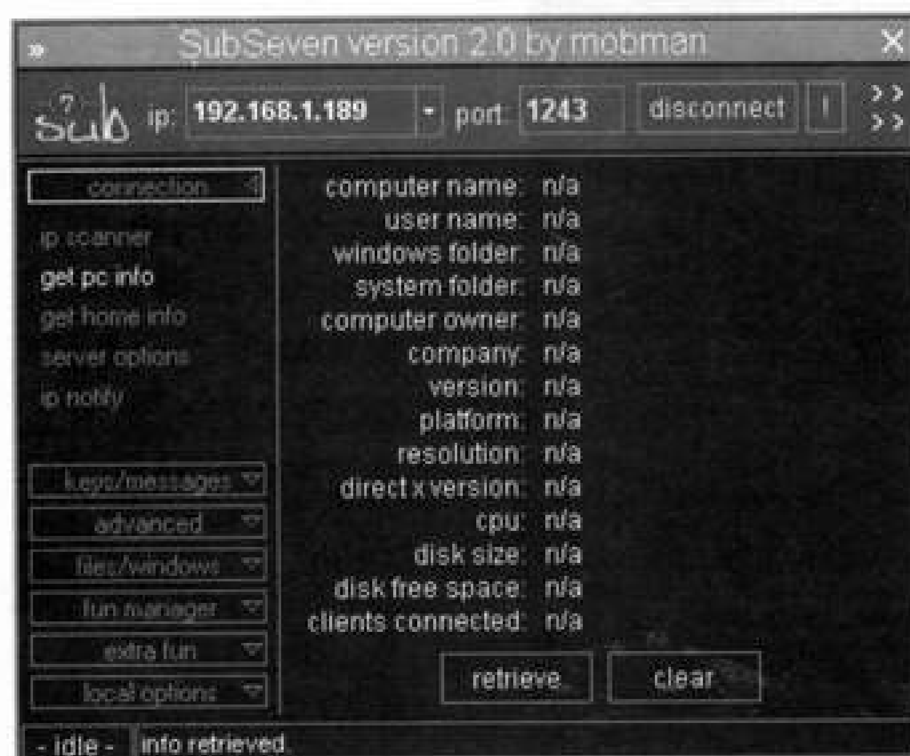
Direct x version = Qual a versão do Direct x.

Cpu = Descrição do processador.

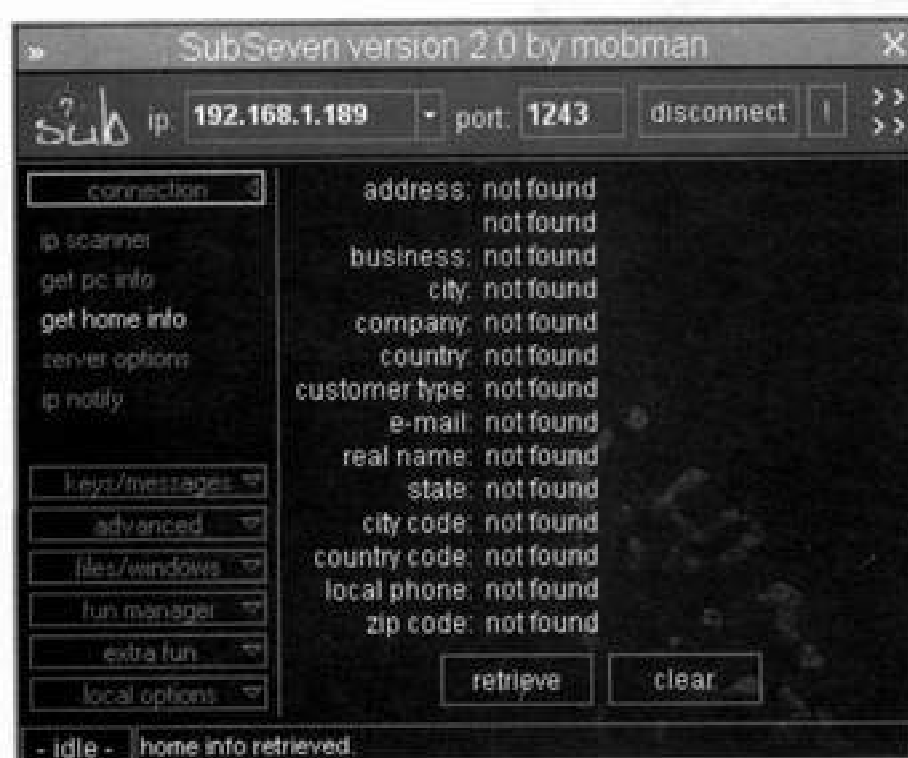
Disk size = Tamanho do disco (HD).

Disk free space = Espaço livre em disco (HD).

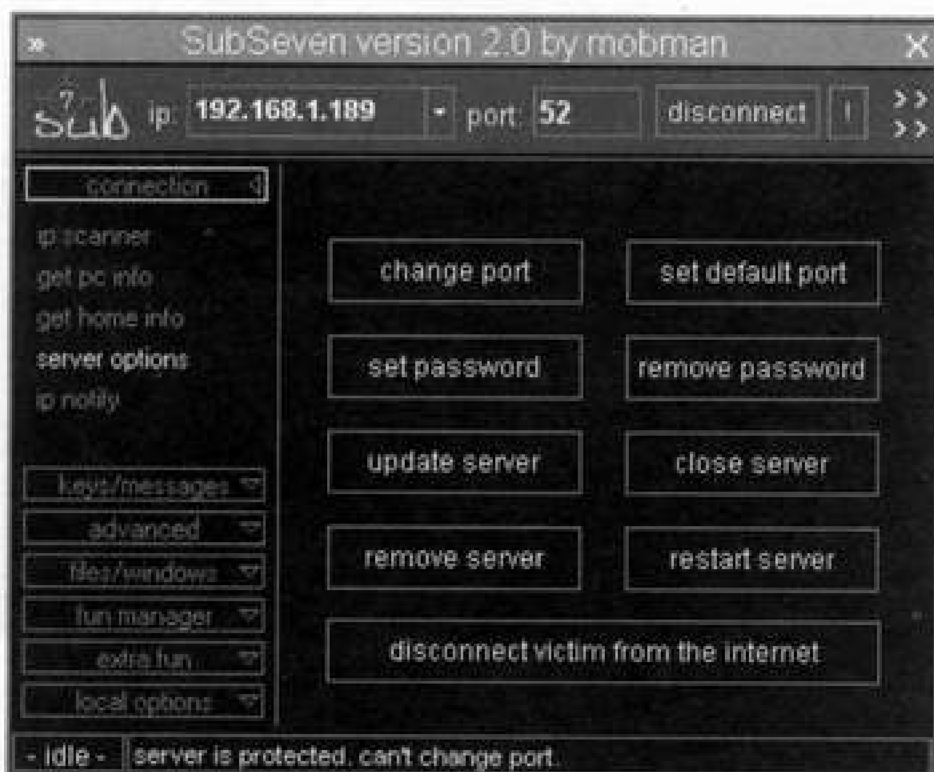
Clients connected = Quantos clientes estão conectados à esta máquina.



3. Get home info: Traz informações pessoais do usuário da máquina.



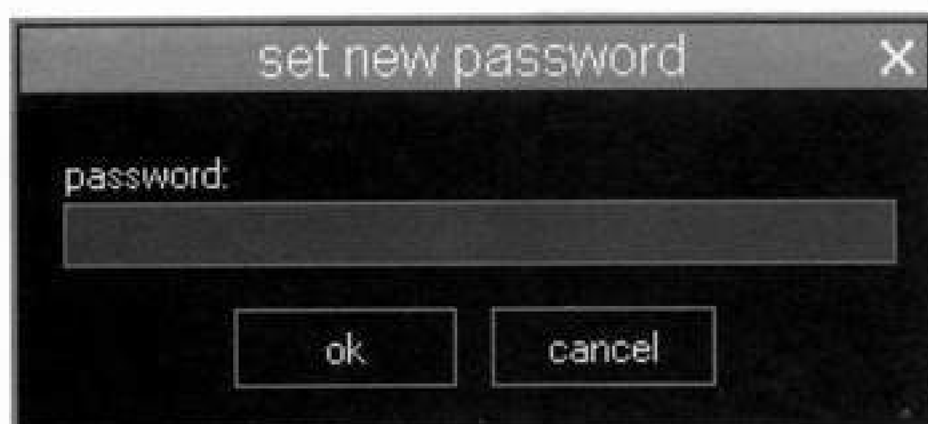
4. Server options: Muda as configurações do server instalado na máquina da vítima.



– Mudar a porta pela qual se conecta, clique em *change port*, coloque o número da nova porta no campo texto e clique em *ok*.



– Adicionar senha, clique em *set password*, digite a senha no campo texto e clique em *ok*.



– Remove a senha do server, clique em *remove password*.

– Atualizar o server, clique em *update server*, selecione o novo server a ser colocado na máquina da vítima e clique em *abrir*.

– Fecha o server e o reinicia. Assim que a máquina for reiniciada, clique em *close server*.

– Para remove definitivamente o server da máquina da vítima. Clique em *remove server*.

– *Restart server*, Reiniciar o server.

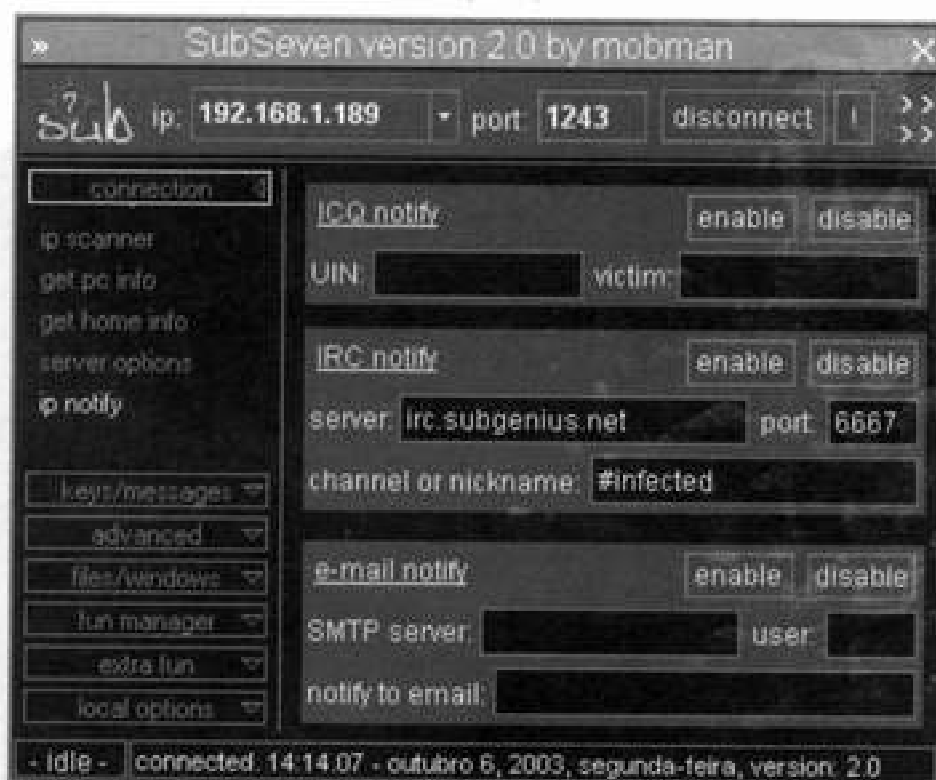
– *Disconnect victim from the internet*, Desconectar a vítima da internet, só funciona quando a conexão é feita por modem, clique em *disconnect victim from the internet*.

5. Ip notify: Notifica o cliente que a vítima está on-line, você pode configurar para ser notificado:

No ICQ, coloque o UIN no campo *UIN* e o nome da vítima no campo *victim*, depois, de preenchido os campos, basta clicar em *enable*.

No IRC, coloque o endereço do *server* no campo *server*, a porta no campo *port*, o canal ou o nickname no campo *channel or nickname*, depois, clique em *enable*.

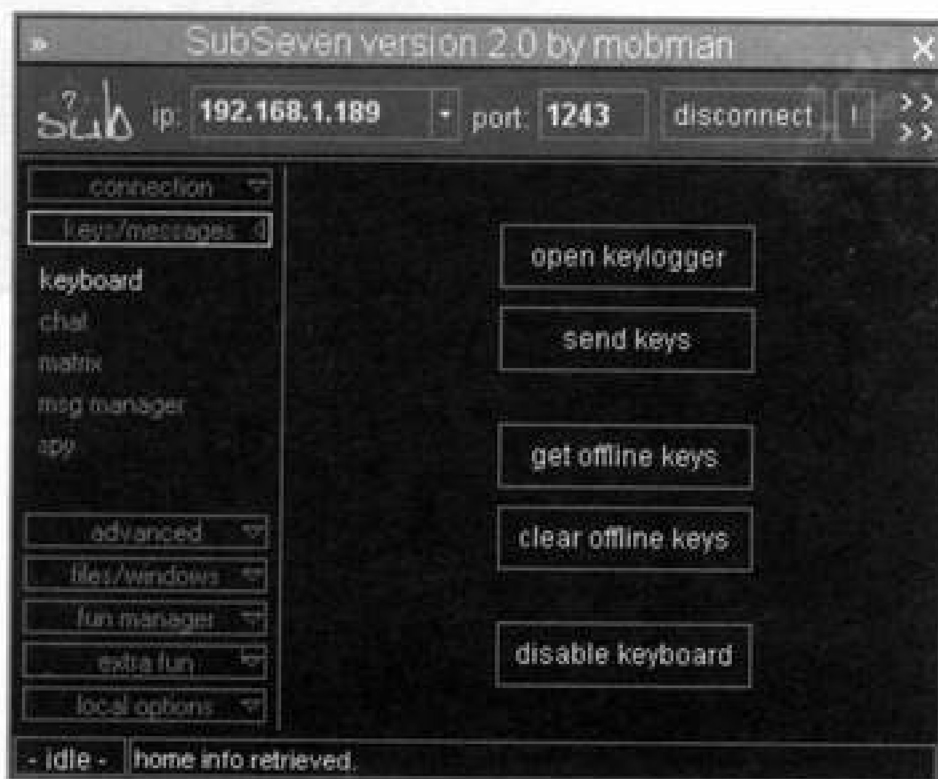
No e-mail, coloca-se o endereço do servidor SMTP em *SMTP server*, o nome do usuário em *user* e o e-mail no campo *notify to email*, depois, clica-se em *enable*.



Clicando na aba *keys/messages*, temos:

1.keyboard
2.Chat
3.Matrix
4.msg manager
5.spy

1. Keyboard: Utilitários relacionados ao teclado.



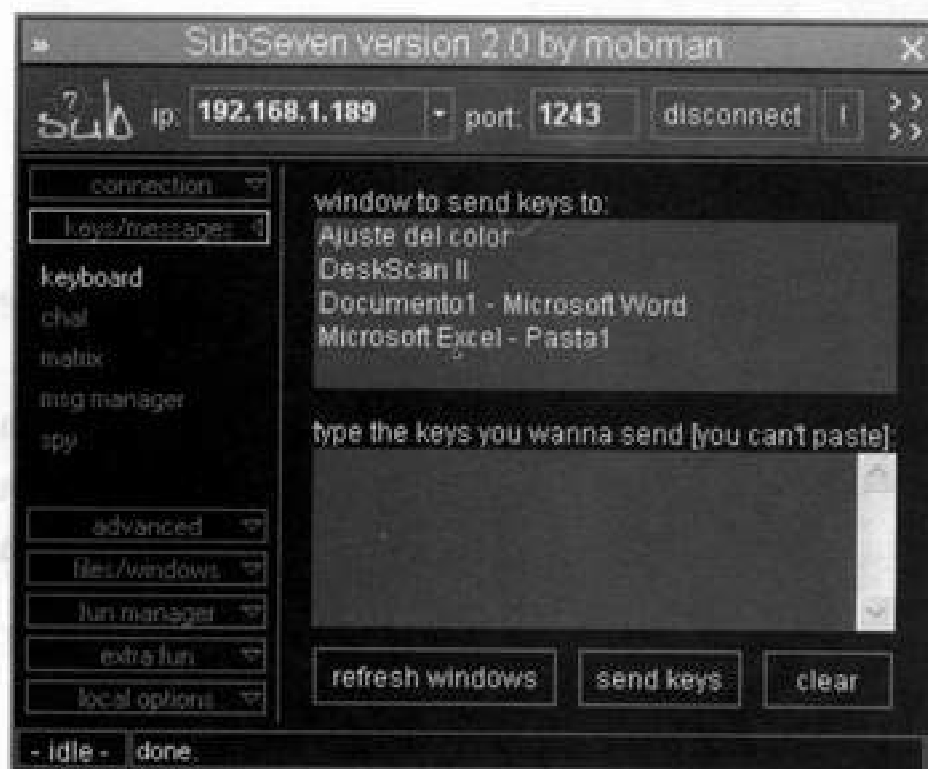
Para capturar as teclas pressionadas na máquina da vítima, clique em *open keylogger*, clique em *start logging*, assim toda tecla pressionada na máquina da vítima aparecerá no quadro.

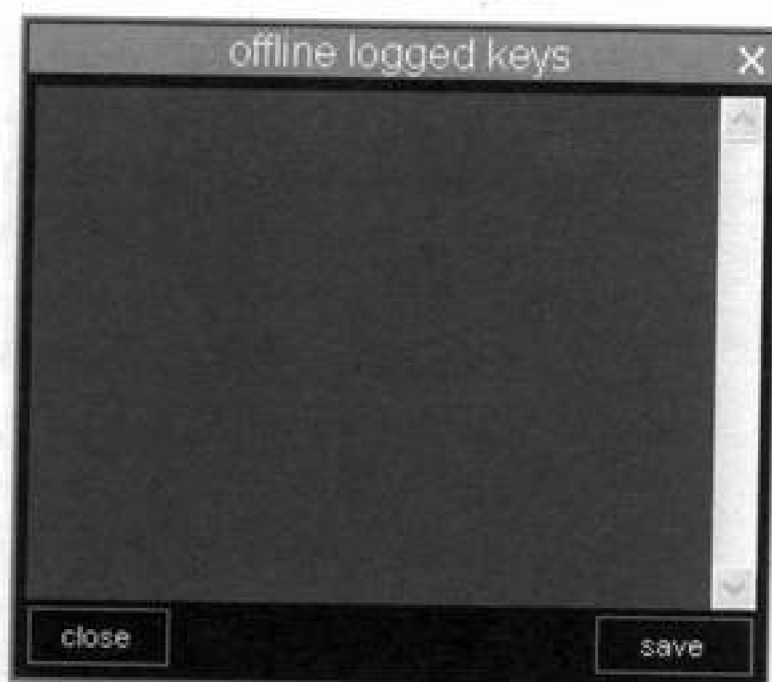


Para enviar caracteres para a vítima, clique em *send keys*, a janela que se abre é dividida em duas. Na parte de cima *window to send keys to*, aparecem os programas que a máquina da vítima está executando. No exemplo abaixo, a vítima está usando quatro programas: um de ajuste de cores; o segundo, um programa de scanner; o terceiro, o Microsoft Word; o último, o Microsoft Excel.

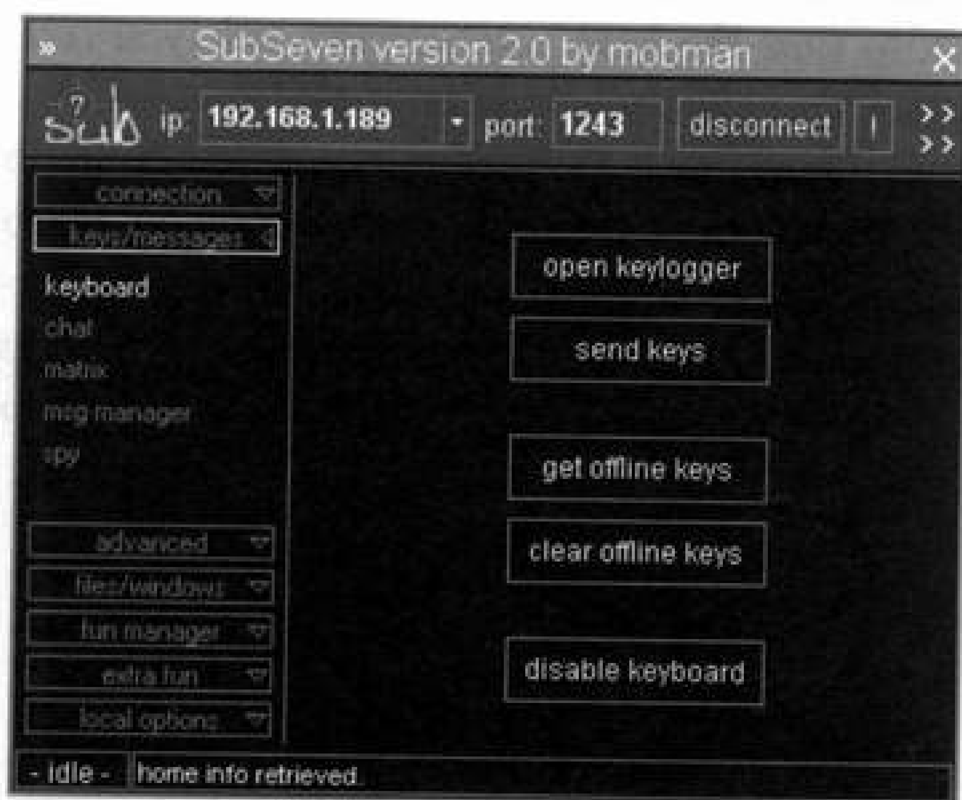
Podemos, no caso citado acima, enviar caracteres para o Word e o Excel por se tratar de programas de edição de arquivos (texto e planilhas de cálculos). Para começar o envio, basta selecionar o programa para o qual devem ser enviados os caracteres clicando em cima do mesmo, depois, no quadro *type the keys you wanna send [you can't paste]*, digite os caracteres a ser enviado, clique em *send keys*.

Pronto! Os caracteres já foram mostrados na máquina da vítima no programa selecionado. É bom lembrar que só se pode enviar texto para programas que recebe caracteres como entrada. Se fossem enviados caracteres para o programa do scanner no caso acima, não obteria nenhum resultado na máquina da vítima, pois o mesmo não foi feito para receber caracteres como entrada.





Para capturar as teclas pressionadas na máquina da vítima enquanto o invasor estiver offline, basta clicar em *get offline keys*. Para apagar o arquivo, clique em *clear offline keys*.



Para desligar o teclado da máquina da vítima, clicar-se em *disable keyboard.*

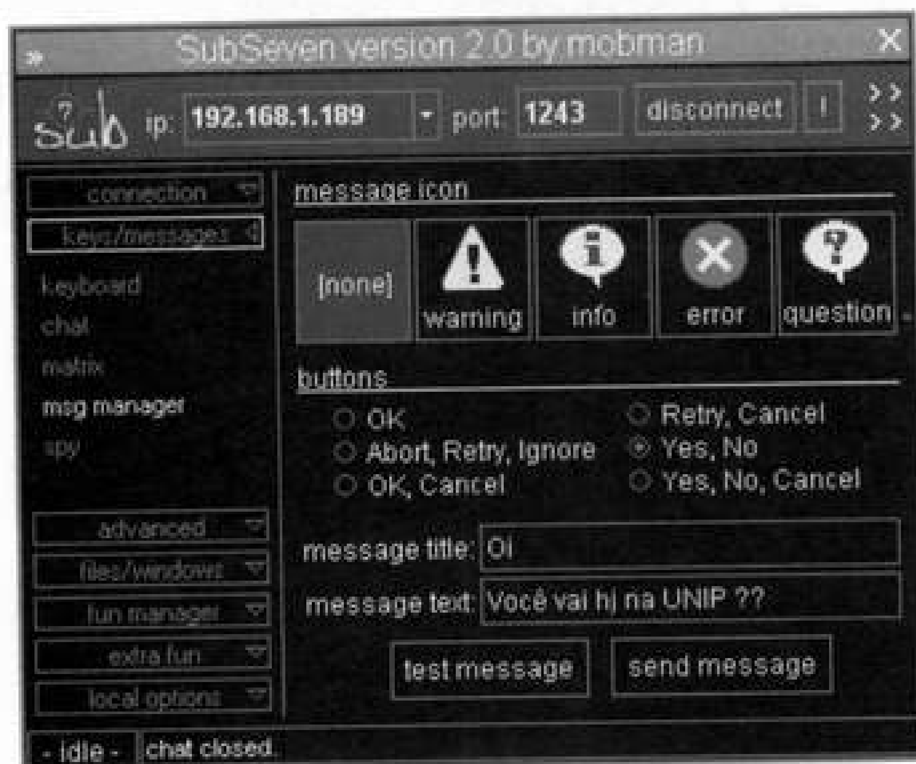
2. Chat: Clicando em *chat with the victim*, é aberto um chat na máquina da vítima, proporcionando a troca de mensagens. Caso haja mais de um cliente conectado à máquina da vítima e o invasor queira trocar mensagens com ele, deve-se clicar em *chat with other clients.*

No campo *nickname for chat*, coloque o nome que você quer usar para trocar mensagens com a vítima.

No campo *victim chat size*, determina o tamanho do chat em porcentagem, logo abaixo, pode-se configurar a cor do texto e o tamanho da fonte tanto para a vítima como para o cliente.



3. Matrix: Abre um chat, mas apenas você pode enviar mensagens para a vítima e ainda desabilita as teclas ctrl+Alt+Del e Alt+Tab.

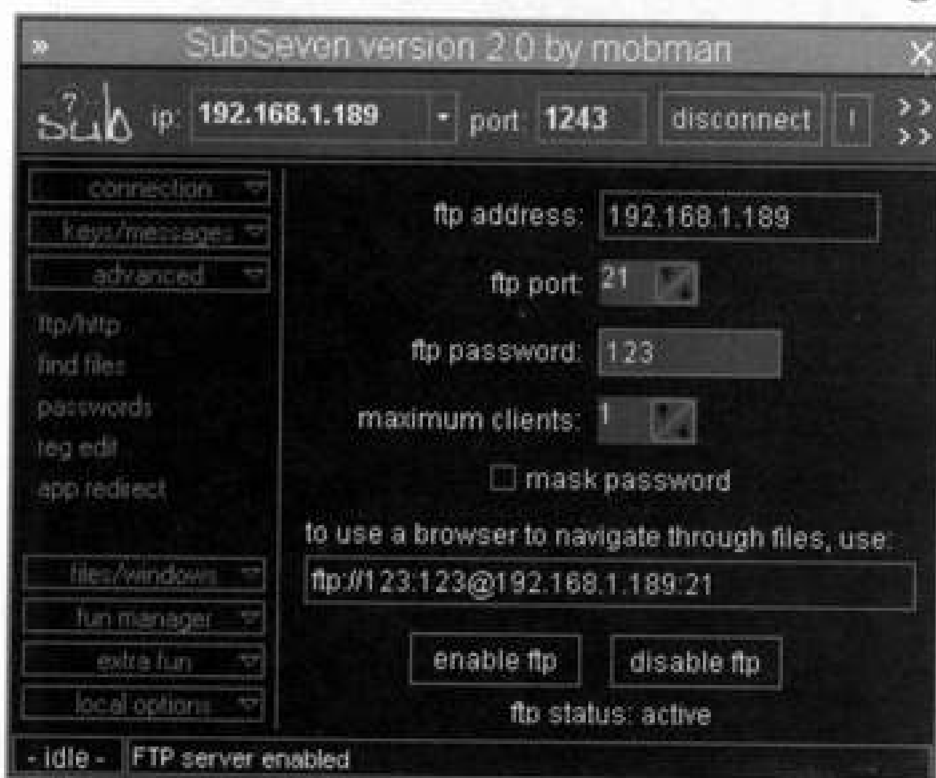


4. msg manager: Envia mensagens de sistema personalizadas para a máquina da vítima. No item *message icon*, você seleciona o ícone que

vai aparecer na mensagem, no item *buttons*, você seleciona os botões que vão na mensagem, no item *message title*, digite o título da mensagem, em *message text*, digite o texto da mensagem, clique em *test message* e você verá como a mensagem vai aparecer na máquina do cliente, e então deve-se, clicar em *send message*.



5. spy: Captura as mensagens recebidas e enviadas para a vítima dos seguintes programas de instant menssenger: ICQ, AOL, MSN, YAHOO, para habilitar o spy de cada *instant messenger*, clique em *enable*.

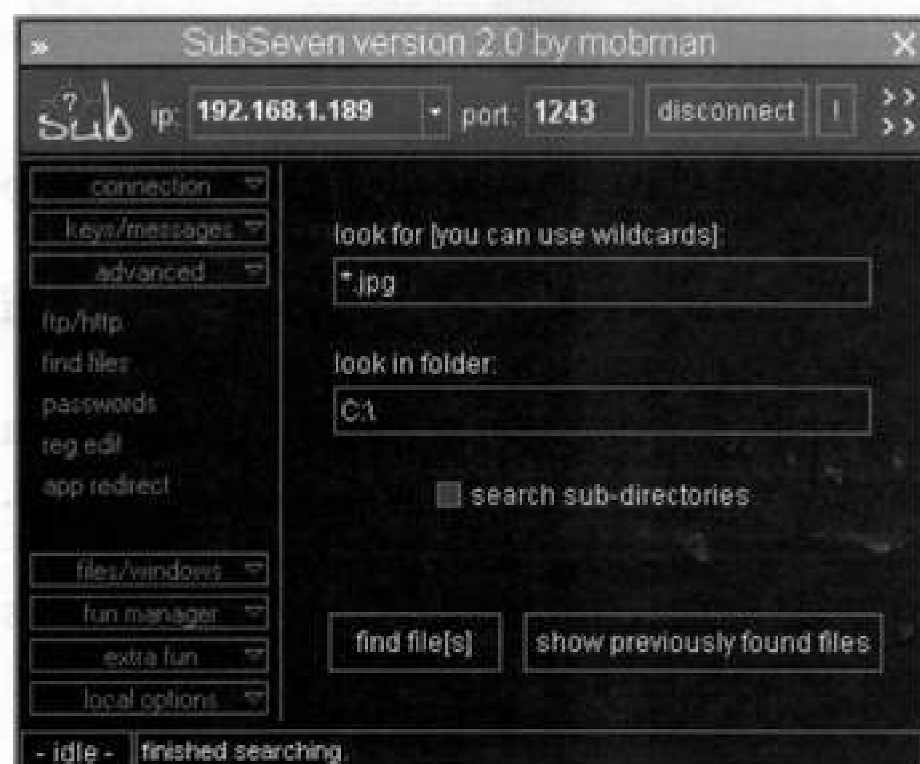


Clicando na aba advanced temos:

1. ftp/http

2. find files
3. Passwords
4. reg edit
5. app redirect

1. ftp/http: Habilita o serviço de ftp na máquina da vítima, possibilitando que acesse os arquivos via browser, usando a seguinte sintaxe: ftp://nome de usuario: senha@ip da máquina alvo. Para habilitar o serviço ftp para a vítima, no campo *ftp address*, coloca-se o ip da máquina da vítima. No campo *ftp port*, deixe a porta default que é a porta 21, mas se quiser você pode alterar. No campo *ftp password*, coloque uma senha para que somente você tenha acesso à máquina da vítima, no campo *maximum clients*, coloque o número máximo de clientes que poderão se conectar à máquina da vítima usando o serviço de ftp, o recomendado é um. Feita as configurações corretas, clique em *enable ftp*. Pronto! Agora, basta copiar o conteúdo do campo *to use a browser to navigate through files, use.* e cole na barra de endereços do browser.



2. find files: Busca arquivos no sistema, semelhante ao pesquisar do Windows. No campo *look for [you can use wildcards]*, deve-se colocar o nome do arquivo a ser buscado, podendo usar o caracter curinga para efetuar a busca no caso a seguir. Ex.: *.jpg vai buscar todos os arquivos cuja a extensão é .jpg. No campo *look in folder*, a seguir deve-se determinar o diretório do qual se deve iniciar a busca, por padrão,

já vem preenchido com o diretório raiz do Windows, no caso, C:\, é aconselhado deixar como está, assim, a busca fica mais abrangente. Para incluir subdiretórios na busca, marque o box *search sub-directories*. Preenchidos os campos, clique em *find files* para iniciar a pesquisa. Caso você tenha feito uma pesquisa e queira ver novamente o resultado obtido na mesma, clique em *show previously found files*.



3. Passwords: Administra as senhas armazenadas no sistema tanto em cache como as armazenadas no disco.

Para visualizar as senhas que estão em cache, clique em *get cached passwords*.

Para visualizar as senhas que estão gravadas no disco da máquina da vítima, clique em *get recorded password*. Para apagar o buffer de senhas, clique em clear *recorded password*.

Para visualizar as senhas do icq ou aim, clique em seus respectivos botões.

4. reg edit: Para editar os registros, basta clicar em *open registry* e efetuar as modificações necessárias.

5. app redirect: Executa comandos do DOS na máquina da vítima e retorna o resultado do comando. No quadro abaixo, pode-se ver o resultado do comando *arp -a*.



Clicando na aba files/windows, temos:

1. file manager
2. Window manager

1. file manager: Ferramenta para edição, execução, remoção e criação de arquivos.

As opções disponíveis nessa ferramenta são:



Refresh: Atualiza os arquivos do diretório corrente.

C: Move do diretório corrente para o C:.

Get drivers: Mostra todos os dispositivos de armazenamento de dados disponíveis na máquina da vítima, como: drivers de CD, disquete e HDs. Selecione o dispositivo a ser acessado e clique em *change to*.

Run: Executa programas na máquina da vítima. Selecione o programa do lado esquerdo e clique em *run* para executá-lo nessa máquina.

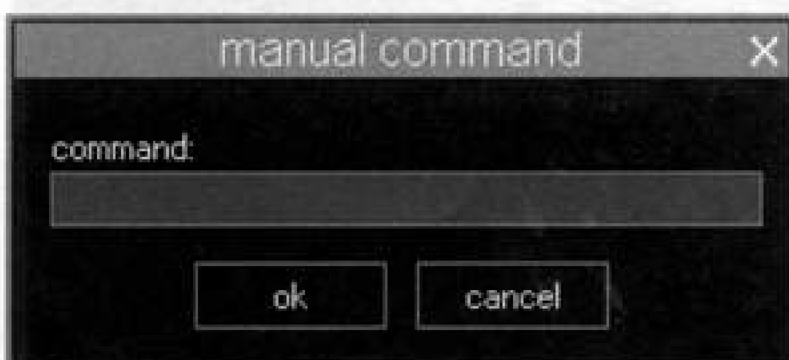


... : Executa comandos do DOS. Para executar o comando, digite o mesmo no campo texto e clique em *ok*.

Type path: Cria o diretório colocado no path.

Download: Baixa o arquivo selecionado para a máquina do invasor.

Get size: Mostra o tamanho do arquivo em bytes.

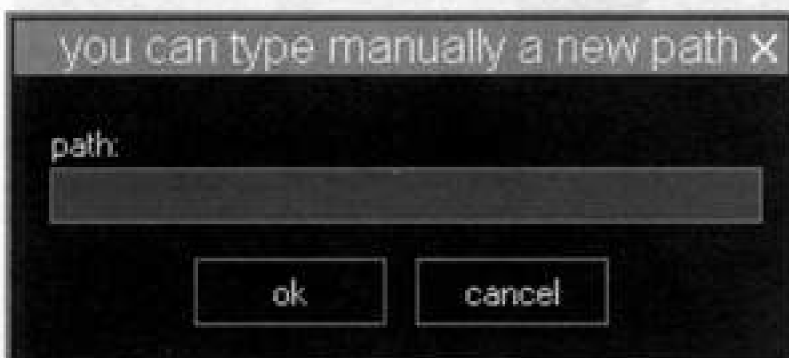


Edit file: Edita arquivos da vítima.

Upload: Envia arquivo para a máquina da vítima.

Delete: Apaga o arquivo selecionado da máquina da vítima.

Play wav: Toca arquivos .wav na máquina da vítima.



Set wallpaper: Modifica o papel de paredes da máquina da vítima, lembrando que aceita apenas .bmp e .jpg. Para modificar, selecione o arquivo e clique em *set wallpaper*.

Print: Imprime arquivos da máquina da vítima na impressora padrão.

2. Window manager: Serve para mostrar todos os processos (programas) que estão sendo executados na máquina da vítima. Para atualizar a lista de processos sendo executados, clique em *refresh*, com a lista atualizada, pode-se dar foco em um determinado processo, dar foco é colocá-lo em primeiro plano. Por exemplo, temos, no quadro abaixo, o word e o excel, a vítima está editando um arquivo no word, mas você dá um foco no excel, automaticamente, o excel fica em primeiro plano e o word vai para segundo plano. Para fazer isso, basta clicar sobre o processo e pressionar o botão *focos*. Para esconder um processo, selecione-o e pressione o botão *hide*, é bom lembrar que, quando você coloca um processo em *hide*, ele não mais fica acessível, nem mesmo na barra de ferramentas. Para mostrá-lo, clique em *show*. Para desabilitar um *processo*, clique em *disable*. Quando você

desabilita um processo, por exemplo: o word, por mais que a vítima digite dentro do word, nada acontece. Esse comando simula um travamento, para habilitá-lo, clique em *enable*.

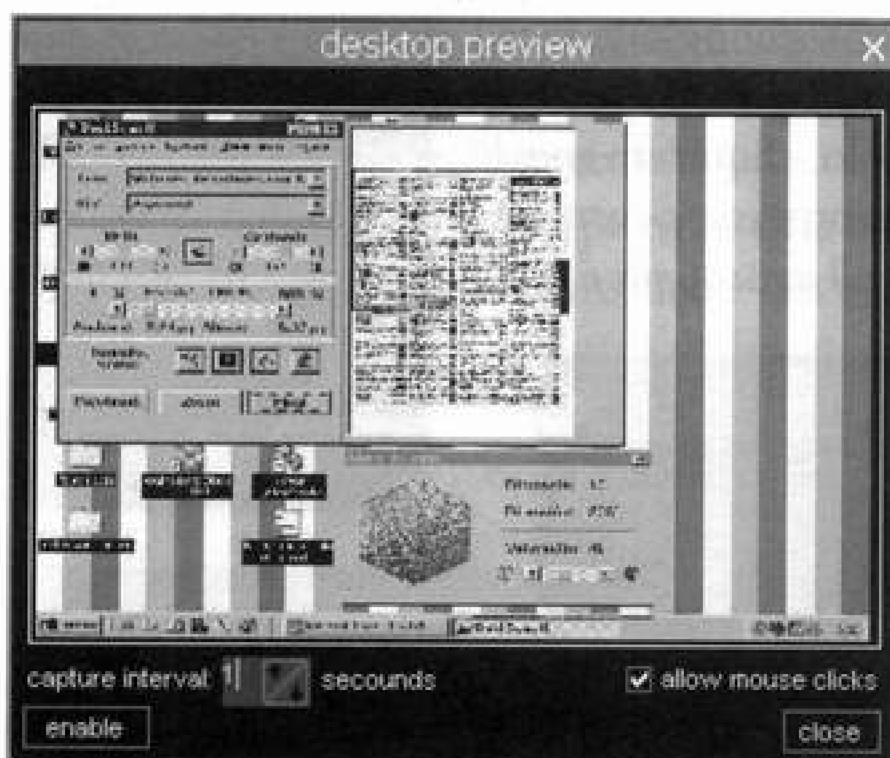
Para visualizar todos os processos correntes na máquina da vítima, marque o quadrado *show all aplications* e, depois, clique em *refresh*.



Clicando na aba *fun manager,* temos:

1. Desktop/webcam
2. Flip screen
3. Print
4. Browser
5. Resolution
6. Win colors

1. Desktop/webcam: Para capturar a tela da máquina da vítima, o invasor deve clicar em *open screen preview*, depois, pressionar o botão *enable* para começar a captura. Deve-se configurar o tempo de intervalo entre uma captura e outra no campo *capture interval*. É possível redimensionar a tela para o tamanho que desejar, para redimensioná-la, basta posicionar o mouse em uma das extremidades da janela, deixar o botão esquerdo pressionado e arrastá-la.

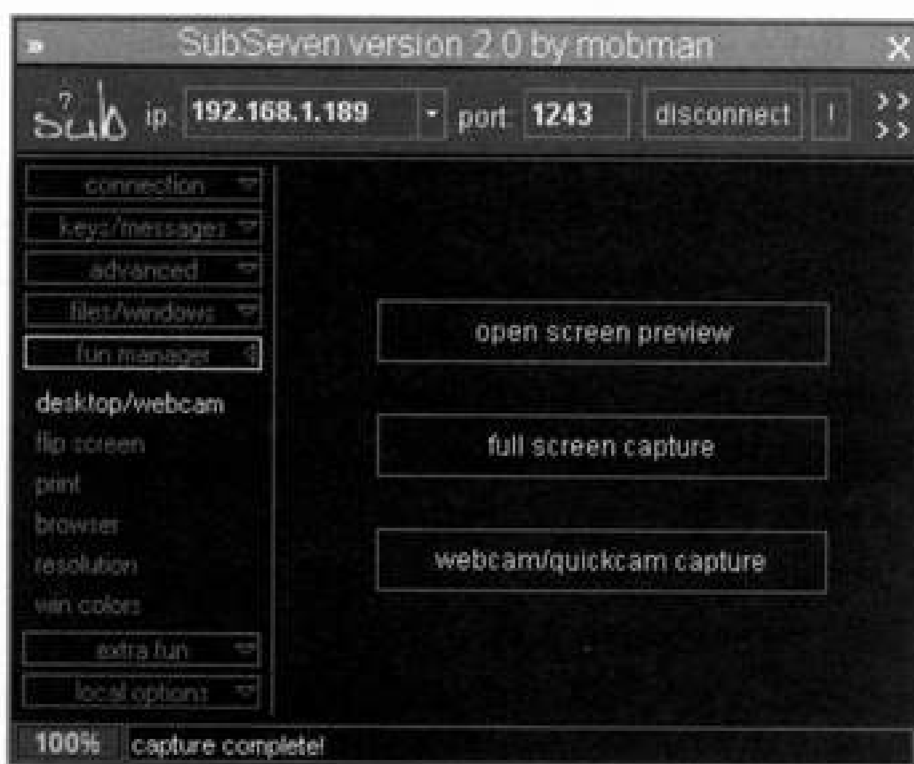


Full screen capture faz a mesma coisa que o citado acima.

Webcam/quickcam capture captura imagens da webcam da máquina da vítima.

2. Flip screen: Inverte a posição da tela na máquina da vítima na vertical e na horizontal. Para inverter, bastar selecionar as opções e clicar em *flip screen*; para inverter na vertical, clique em *flip screen vertically*; para inverter na horizontal, em *flip screen horizontally*, feita as opções clique em *flip screen*.

3. Print: Envia para a impresora da máquina da vítima o texto digitado no box. Após digitar o texto no box deve-se fazer as configurações necessárias e então clicar em *print text*.





4. Browser: Abre o navegador padrão na máquina da vítima com a url colocada no campo texto.

Para efetuar essa operação, coloque a url no campo texto e clique em *open browser*.

5. Resolution: Modifica a resolução atual da máquina da vítima. Para fazer a modificação, clique em *refresh*, selecione a resolução desejada e, posteriormente, clique em *change*.



6. Win colors: Muda as cores dos objetos do Windows, como: menus, botões etc. Para efetuar a mudança, selecione as cores desejadas para os objetos e clique em *test colors* para ver o resultado. Caso seja o esperado,

clique em *change colors* para modificar na máquina da vítima. Para restaurar as cores originais, clique em *restore default colors*.



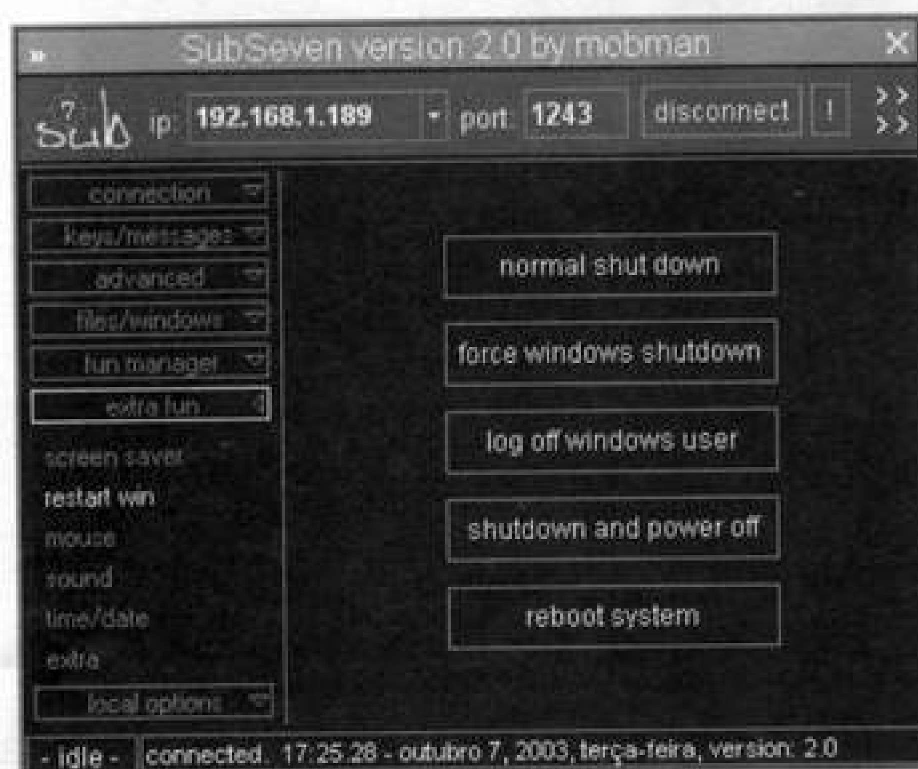
Clicando na aba *extra fun*, temos:

1. Screen saver
2. Restart win
3. Mouse
4. Sound
5. Time/date
6. Extra

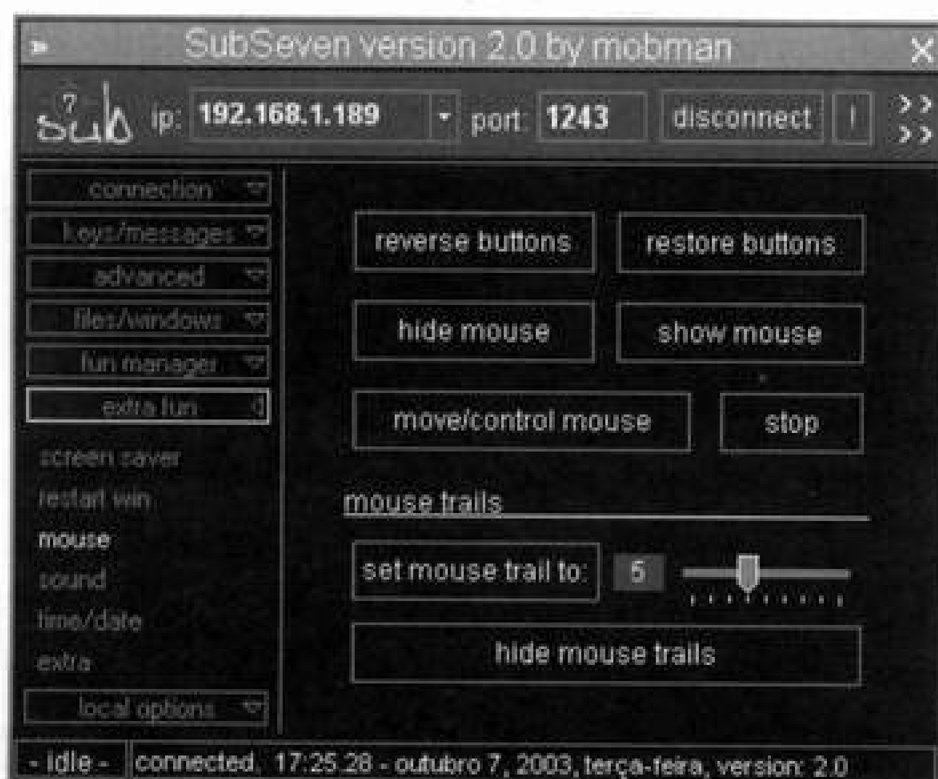
1. Screen saver: Executa o screen saver na máquina da vítima, com o texto digitado no campo *text*, a fonte selecionada no campo *font*, o tamanho colocado no campo *size* e as outras configurações feitas.



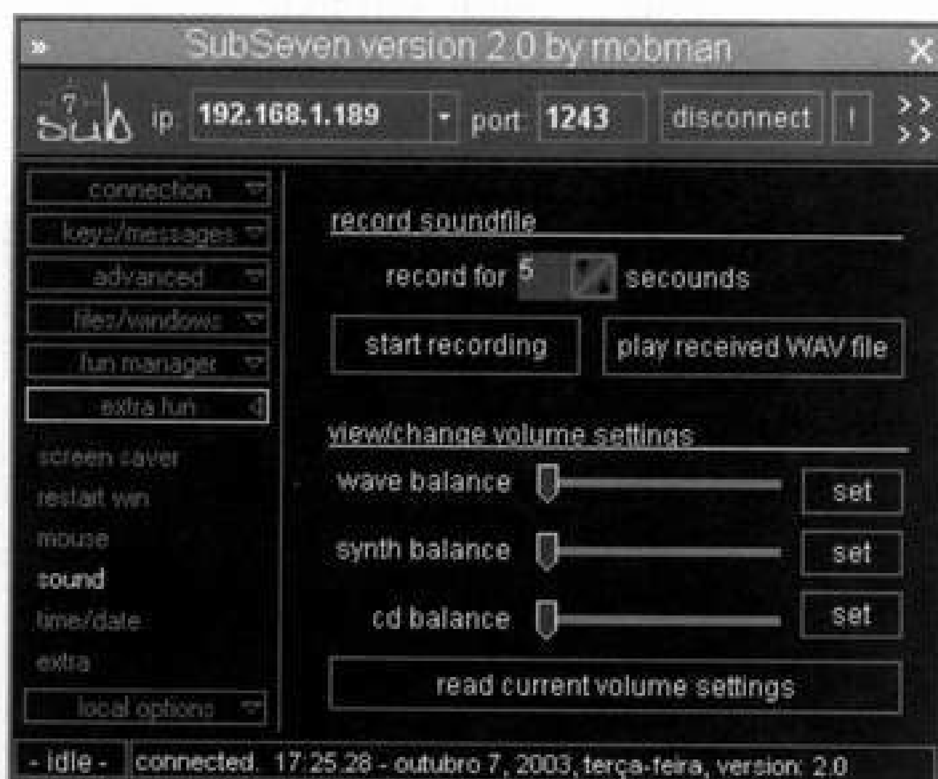
2. Restart win: Para desligar a máquina normalmente, clique em *normal shutdown*. Para forçar o desligamento, clique em *force Windows shutdown*. Para dar logoff no usuário atual, clique em *log off Windows user*. Para desligar a máquina e o monitor, clique em *shutdown and power off*. Para reiniciar o sistema, clique em *reboot system*.



3. Mouse: Ferramentas para manuseio do mouse. Para inverter os botões do mouse, clique em *reverse buttons*; para restaurar os botões, em *restore buttons*. Para ocultar o mouse, clique em *hide mouse*; para mostrá-lo, vá em *show mouse*. Para mover o mouse, clique em *move/control mouse* e mova o mouse. Na máquina da vítima, os movimentos feitos por você são simulados. Ainda é possível pode habilitar a sombra do mouse clicando em *set mouse trail to*, para desabilitar, clique em *hide mouse trails*.

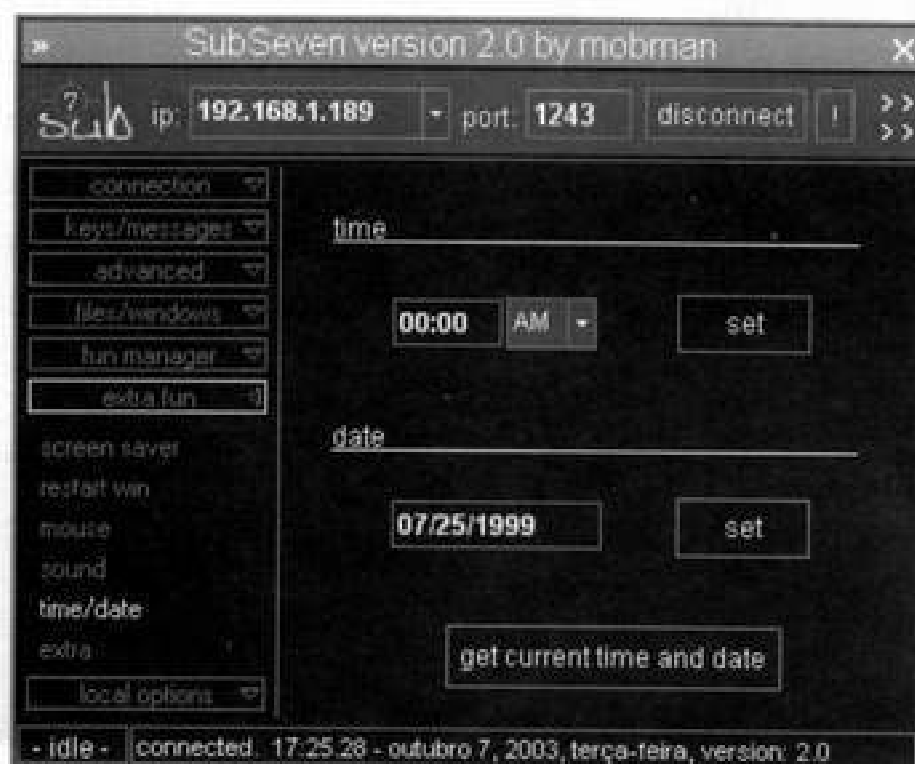


4. Sound: Ferramentas para manipulação e configuração do som. Para gravar pelo microfone da máquina da vítima o que ela está conversando, por exemplo, clique em *start recording*. Para tocar o que foi gravado, clique em play *received WAV file*. Para alterar as configurações de som, abaixo de *view/change volume settings*. Para aumentar o volume, arraste o ponteiro para a direita, para diminuir, arraste para a esquerda. Escolhido o volume, clique em *set*. Para visualizar as configurações de volume atuais, clique em *read current volume settings*.



5. Time/date: Modifica a hora e a data da máquina da vítima. Para alterar a hora, basta preencher o campo *texto*, abaixo do item *time*, e

clicar em *set*; para a data, siga o mesmo procedimento só que no item *date*. Para visualizar a configuração atual, clique em *get current time and date*.



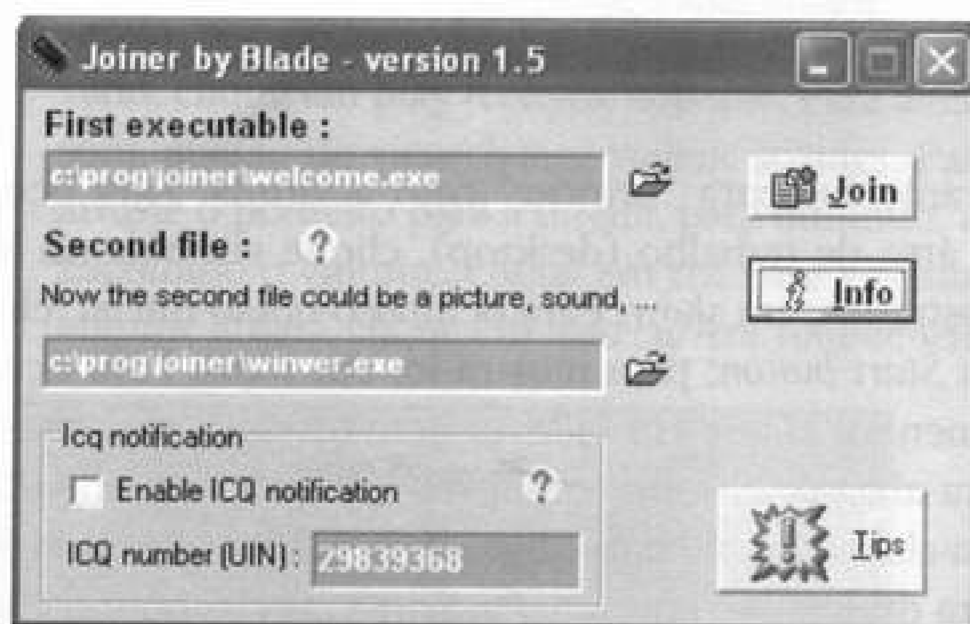
6. Extra: Ferramentas para "brincar" com a vítima. Para ocultar todos ícones da área de trabalho (desktop), clique em *hide* no item *desktop*; para mostrá-los, em *show*. Para ocultar o botão iniciar, clique em *hide* no item *Start button*; para mostrá-lo, em *show*. Para ocultar a barra de ferramentas, clique em *hide* no item *taskbar*; para mostrá-la, em *show*. Para abrir o cd rom, clique em *open* no item *CD ROM*; para fechá-lo, em *close*. Para ligar as caixas de som, clique em *start* no item *speaker*; para desligá-las, em *stop*. Para desligar o monitor, clique em *off* no item *monitor*; para ligá-lo, em *on*. Para desabilitar as teclas Ctrl+Alt+Del, clique em *off* no item *Ctrl+Alt+Del*; para habilitá-las, em *on*. Para ligar a tecla Scroll Lock, clique em *on* no item *Scroll Lock*; para desligá-la, em *off*. Para ligar a tecla Caps Lock, clique em *on* no item *CapsLock*; para desligá-la, em *off*. Para ligar a tecla Num Lock, clique em *on* no item *NumLock*; para desligá-la, em *off*.

Joiner 1.5

O joiner é um programa usado para mesclar um arquivo executável a um arquivo de imagem ou mesmo um arquivo de som. Quando a pessoa clica no .exe, na verdade, será executado o arquivo mesclado,

por exemplo, temos o server gerado no exemplo do subseven, para mesclá-lo com uma imagem, seguiríamos os seguintes passos no campo *First executable*: deve ser aberto o arquivo do server no caso do subseven, para fazer isso, clique no ícone *pasta*, que se encontra na frente do campo, selecione o arquivo e clique em *abrir*. No campo *Second file*, você deve abrir a imagem, o som ou mesmo um arquivo Word, Excel etc. Selecionado os arquivos, clique em *join* e será gerado um arquivo RESULT.exe no diretório do joiner, uma técnica muito usada é colocar um .jpg e acrescentar espaços em branco entre o .jpg e o .exe.

Ex.: loira.jpg   .exe . Se você mesclou o server com uma foto, ao se executar o arquivo, a vítima visualizará a foto, e arquivos de imagens não possuem extensão .exe.





Expediente

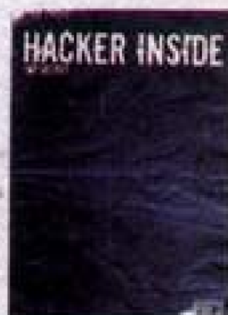
Papel
Capa: Triplex 250g;
Miolo: Sulfite 70 g.

Tipografia
Berkeley (Adobe);
Helvetica (Adobe);
Downcome (www.misprintedtype.com).



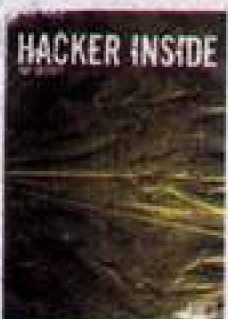
EDITORA GRÁFICA TERRA LTDA.
Av. Caiapó nº 758 – Setor Santa Genoveva
CEP: 74672-400 – Goiânia-GO – Brasil
Tel: (62) 4005-9000 – Fax: (62) 207-1666
Televendas: (62) 4005-9090
e-mail: info@editoraterra.com.br

VOCÊ ACHA QUE JÁ APRENDEU TUDO? ESTÁ ENGANADO. ESTE É SÓ O BÁSICO QUE OS HACKERS PODEM FAZER COM UM SISTEMA. CONFIRA AS PRÓXIMAS EDIÇÕES!



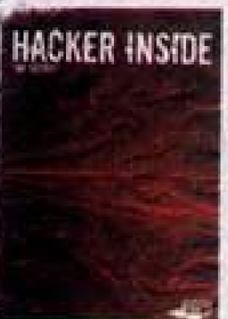
FASCÍCULO 02
Espionagem – Keylogger
Fundamentos de esteganografia, criptografia, criptoanálise
Pesquisa de informações – Search engines, alvos distantes
Proteção: Firewalls, antivírus
Senha

E MAIS... UM DESAFIO HACKER! VOCÊ TERÁ DE ACESSAR UM SISTEMA E DESCOBRIR SUAS FALHAS. AS PRIMEIRAS FASES EXPLICADAS PASSO A PASSO.



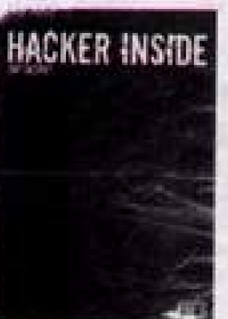
FASCÍCULO 03
Sniffing
Scripts
Linux x Instalação e comandos básicos
Anonimato, utilização do proxy
Tunneling

MAIS DESAFIO HACKER... A BRINCADEIRA ESTÁ SÓ COMEÇANDO.



FASCÍCULO 04
Cookies: Alterações de dados
Mapeamento de rede
DNS queries
PHP: Falhas e exploits
Spoofing e Scanning

DESAFIO HACKER – NÍVEL AVANÇADO



FASCÍCULO 05

TOP SECRET


ISBN: 85-7491-166-6
9 788574 911663 >


EDITORA
TERRA

Visite nosso site:

www.cursodehacker.com.br